

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-2008-AVI-277>

---

### Gestion du document

|                             |                                 |
|-----------------------------|---------------------------------|
| Référence                   | CERTA-2008-AVI-277-001          |
| Titre                       | Vulnérabilités dans OpenSSL     |
| Date de la première version | 29 mai 2008                     |
| Date de la dernière version | 27 juin 2008                    |
| Source(s)                   | Bulletin OpenSSL du 28 mai 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.

## 2 Systèmes affectés

*OpenSSL*, version 0.9.8g et versions antérieures.

## 3 Résumé

Deux vulnérabilités dans *OpenSSL* permettent à un utilisateur malveillant de provoquer un déni de service à distance.

## 4 Description

La première vulnérabilité concerne les versions du logiciel *OpenSSL* compilées en utilisant, pour les noms de serveurs TLS, des extensions qui ne sont pas les extensions par défaut. Par le biais d'un paquet conçu à cet effet, un utilisateur malveillant peut provoquer un arrêt inopiné (*crash*) du programme.

La deuxième vulnérabilité est relative à la négociation en début de session TLS. Si un client se connecte avec certaines options cryptographiques sur un serveur malveillant, ce dernier peut provoquer un arrêt inopiné (*crash*) du client.

## 5 Solution

La version 0.9.8h résout ces problèmes.

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

## 6 Documentation

- Bulletin de sécurité du projet OpenSSL du 28 mai 2008 :  
[http://www.openssl.org/news/secadv\\_20080528.txt](http://www.openssl.org/news/secadv_20080528.txt)
- Bulletin de sécurité Nortel 2008009822 du 25 juin 2008 :  
<http://support.nortel.com/go/main.jsp?cscat=BLTDETAIL&id=738400>
- Bulletin de sécurité Nortel 2008009823 du 25 juin 2008 :  
<http://support.nortel.com/go/main.jsp?cscat=BLTDETAIL&id=738962>
- Référence CVE CVE-2008-0891 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0891>
- Référence CVE CVE-2008-1672 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1672>

## Gestion détaillée du document

**29 mai 2008** version initiale.

**27 juin 2008** ajout des références aux bulletins de sécurité Nortel.