

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Faille dans l'implémentation d'OpenSSL sous Microsoft Windows

---

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-2003-AVI-179>

---

### Gestion du document

Référence	CERTA-2003-AVI-179-001
Titre	Faille dans l'implémentation d'OpenSSL sous Microsoft Windows
Date de la première version	05 novembre 2003
Date de la dernière version	06 novembre 2003
Source(s)	Avis de sécurité du NISCC 006489/OpenSSL2/1
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.

## 2 Systèmes affectés

OpenSSL version 0.9.6k sur Microsoft Windows.

## 3 Résumé

Un utilisateur mal intentionné peut provoquer un déni de service sur une machine qui utilise une version d'OpenSSL vulnérable.

## 4 Description

OpenSSL est une mise en œuvre « *open source* » des protocoles *Secure Sockets Layer* (SSL) et *Transport Layer Security* (TLS). OpenSSL est largement utilisé pour sécuriser des protocoles applicatifs sur l'Internet.

Les protocoles SSL et TLS utilisent le langage Abstract Syntax Notation One (ASN.1) dans les échanges de certains objets.

Une vulnérabilité dans le traitement d'un objet ASN.1 permet à un utilisateur mal intentionné de provoquer un déni de service, en envoyant par exemple un certificat mal formé à un serveur vulnérable.

## **5 Solution**

Mettre à jour OpenSSL (version 0.9.7c ou 0.9.6l).

## **6 Documentation**

Avis de sécurité 006489/OpenSSL2/1 du NISCC (National Infrastructure Security Co-ordination Center) :  
<http://www.uniras.gov.uk/vuls/2003/006489/openssl2.htm>

Référence CVE CAN-2003-0851 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0851>

Avis de sécurité d'OpenSSL (Denial of service in ASN.1 parsing) :  
[http://www.openssl.org/news/secadv\\_20031104.txt](http://www.openssl.org/news/secadv_20031104.txt)

## **Gestion détaillée du document**

**05 novembre 2003** version initiale.

**06 novembre 2003** première révision : correction du titre.