



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 1er avril 2003  
N° CERTA-2003-AVI-057-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Failles dans des implémentations de SSL/TLS

---

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-057>

---

### Gestion du document

Référence	CERTA-2003-AVI-057-001
Titre	Failles dans des implémentations de SSL/TLS
Date de la première version	25 mars 2003
Date de la dernière version	1er avril 2003
Source(s)	-
Pièce(s) jointe(s)	Aucune

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Risque

- Atteinte à la confidentialité des sessions ;
- usurpation d'identité.

## 2 Systèmes affectés

- Tout système utilisant les fonctions de la bibliothèque *openssl* jusqu'aux versions 0.9.7a et 0.9.6i (en particulier le module *mod\_ssl* du serveur web *Apache* et l'application *Stunnel*) ;
- tout programme utilisant la bibliothèque *Crypto++* ;
- tout programme utilisant les kits de développement "SSH IPSEC Express" et "SSH Certificate/TLS" de la société *SSH communications Security* ;
- tout système utilisant *OpenSSH* dans une version antérieure à la 3.6.

## 3 Résumé

Deux failles, présentes dans certaines implémentations des protocoles SSL/TLS, permettent à un utilisateur mal intentionné soit de récupérer la clé secrète d'un serveur, soit le secret partagé d'une session client/serveur.

## 4 Description

Des travaux de recherche sur les implémentations des protocoles SSL/TLS ont démontré de nouvelles sources de vulnérabilité :

- En ouvrant de très nombreuses sessions avec serveur et en utilisant des contenus chiffrés habilement choisis, il est possible d’obtenir le chiffrement/déchiffrement d’un texte arbitraire par la clé privée RSA du serveur. Cela peut alors permettre de déchiffrer une session interceptée ou d’usurper l’identité du serveur.
- Moyennant une certaine proximité, il est possible de déterminer la clé privée d’un serveur en mesurant ses temps de réponse. La plupart des implémentations matérielles et la bibliothèque *NSS* du navigateur *Mozilla* ne semblent pas vulnérables.

## 5 Solution

- Mettre à jour les sources de la bibliothèque *OpenSSL* :  
[http://www.openssl.org/news/secadv\\_20030317.txt](http://www.openssl.org/news/secadv_20030317.txt)  
[http://www.openssl.org/news/secadv\\_20030319.txt](http://www.openssl.org/news/secadv_20030319.txt)
- Mettre à jour la bibliothèque *Crypt++* en version 5.1 au moins :  
<http://www.eskimo.com/~weidai/cryptlib.html>
- Mettre à jour les programmes/modules suivants :
  - *Stunnel* :  
<http://marc.theaimsgroup.com/?l=stunnel-users&m=104827610907579&w=2>
  - *mod\_ssl* pour serveur web *Apache* :  
<http://marc.theaimsgroup.com/?l=apache-modssl&m=10480002921649&w=2>
  - *OpenSSH* :  
<http://www.openssh.com>
- Appliquer le correctif du vendeur :
  - OpenBSD :  
<http://www.openbsd.com/errata.html>
  - FreeBSD :  
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-03:06.openssl.asc>
  - NetBSD :  
<ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-007.txt.asc>
  - MacOSX :  
<http://docs.info.apple.com/article.html?artnum=120199>
  - IBM “AIX Toolbox for Linux” *OpenSSL* et *mod\_ssl* :  
<http://www6.software.ibm.com/dl/aixtbx/aixtbx-p>
  - OpenPKG :  
<http://www.openpkg.org/security/OpenPKG-2003.026-openssl.html>
  - SCO OpenLinux :  
<ftp://ftp.sco.com/pub/security/OpenLinux/CSSA-2003-014.0.txt>
  - Gentoo Linux :  
<http://forums.gentoo.org/viewtopic.php?t=43709>
  - Trustix Secure Linux :  
<http://www.trustix.net/errata/misc/2003/TSL-2003-0010-openssl.asc.txt>
  - Engarde Secure Linux :  
[http://www.linuxsecurity.com/advisories/engarde\\_advisory-3009.html](http://www.linuxsecurity.com/advisories/engarde_advisory-3009.html)

## 6 Documentation

- Réponse de la société *SSH Communications Security* au CERT/CC :  
<http://www.kb.cert.org/vuls/id/AAMN-5KR27C>
- Attaque sur le chiffrement RSA :
  - “Attacking RSA-based Sessions in SSL/TLS” par V. Klima, O. Pokorny et T. Rosa :  
<http://eprint.iacr.org/2003/052/>
  - Référence CVE CAN-2003-0131 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0131>
- Attaque sur les temps de calcul :
  - “Remote Timing Attacks are Practical” par D. Brumley et D. Boneh :  
<http://crypto.stanford.edu/dabo/papers/ssl-timing.pdf>
  - Référence CVE CAN-2003-0147 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0147>

### Gestion détaillée du document

**25 mars 2003** version initiale ;

**1er avril 2003** ajout des systèmes AIX et NetBSD, des bibliothèques de *SSH Communications Security* et *Crypto++*, et des produits *Stunnel*, *OpenSSH* et *mod\_ssl*.