

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-156>

---

### Gestion du document

Référence	CERTA-2003-AVI-156-007
Titre	Failles dans des implémentations de SSL/TLS
Date de la première version	30 septembre 2003
Date de la dernière version	11 mars 2004
Source(s)	Avis de sécurité du NISCC
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

- Dénis de service ;
- Exécution de code arbitraire à distance.

## 2 Systèmes affectés

Tout système utilisant *OpenSSL* pour implémenter les protocoles de session SSL et TLS. En particulier le module *mod\_ssl* d'*Apache* ou les implémentations TLS des serveurs de messagerie *Sendmail*, *Postfix*, *Qmail*,... et les services POP ou IMAP sécurisés par *Stunnel* sont impactés.

## 3 Résumé

Un utilisateur mal intentionné peut transmettre un certificat volontairement mal formé qui entraînera un déni de service ou l'exécution de code arbitraire sur l'hôte destinataire.

## 4 Description

Les certificats, utilisés par les protocoles SSL/TLS, sont des structures codées à l'aide d'un langage standard, ASN.1 (Abstract Syntax Notation One). Lors du traitement de données ne respectant volontairement pas les règles de ce langage, le décodeur peut mal gérer l'information reçue.

Trois vulnérabilités associées ont été découvertes dans *OpenSSL* :

- l'usage d'une balise ASN.1 peu usitée peut provoquer un accès mémoire incohérent engendrant un déni de service (références CAN-2003-0543 et CAN-2003-0544) ;
- une clé publique invalide peut arrêter inopinément le décodeur lorsqu'il lui est spécifié d'ignorer les erreurs (configuration employée en test et non en production) ;
- des structures ASN.1 rejetées comme invalides provoquent de mauvaises gestions de la mémoire qui pourraient être exploitées pour exécuter du code arbitraire à distance (référence CAN-2003-0545).

Par ailleurs, un mauvais respect des spécifications SSLv3 et TLS fait qu'un serveur utilisant *OpenSSL* accepte les certificats client lorsqu'ils ne sont pourtant pas sollicités. Cela offre l'opportunité d'exploiter les failles décrites ci-dessus.

## 5 Solution

Mettre à jour *OpenSSL*.

- Code source d'*OpenSSL* en versions 0.9.6l ou 0.9.7c au moins :  
<http://www.openssl.org>
- Linux Red Hat :  
<https://rhn.redhat.com/errata/RHSA-2003-290.html>  
<https://rhn.redhat.com/errata/RHSA-2003-291.html>  
<https://rhn.redhat.com/errata/RHSA-2003-292.html>  
<https://rhn.redhat.com/errata/RHSA-2003-293.html>
- Mandrake Linux :  
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:098>
- Slackware Linux :  
<http://slackware.com/security/viewer.php?l=slackware-security&y=2003&m=slackware-security.464492>
- SuSE Linux :  
[http://www.suse.com/de/security/2003\\_043\\_openssl.html](http://www.suse.com/de/security/2003_043_openssl.html)
- Debian GNU/Linux :  
<http://www.debian.org/security/2003/dsa-393>
- Apple MacOS X :  
<http://docs.info.apple.com/article.html?artnum=61798>
- OpenBSD :  
<http://www.openbsd.com/errata.html#asn1>
- FreeBSD :  
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-03:18.openssl.asc>
- NetBSD :
  - OpenSSL versions 0.9.7 :  
<ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-017.txt.asc>
  - OpenSSL versions 0.9.6 :  
<ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-003.txt.asc>
- SGI Irix :  
<ftp://patches.sgi.com/support/free/security/advisories/20030904-01-P.asc>
- HP-UX :
  - Serveur web *Apache* :  
<http://www4.itrc.hp.com/service/cki/docDisplay?docId=HPSBUX0310-284>  
<http://www4.itrc.hp.com/service/cki/docDisplay?docId=HPSBUX0310-285>

- “AAA Server” :  
<http://www4.itrc.hp.com/service/cki/docDisplay?docId=HPSBUX0310-286>
- “HP WBEM Services” :  
<http://www4.itrc.hp.com/service/cki/docDisplay?docId=HPSBUX0310-288>
- Cisco :  
<http://www.cisco.com/warp/public/707/cisco-sa-20030930-ssl.shtml>
- Stunnel :  
<http://www.stunnel.org>
- Nortel Networks “Alteon Switched Firewall”, “Alteon iSD - SSL Accelerator”, CallPilot, Contivity, “Succession Communication Server 2000 - Compact” et “Preside Service Provisioning” :  
Contacter le revendeur.
- Sun Linux et Cobalt :  
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57100>
- SunPlex (Sun Cluster) :  
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57475>
- Sun Java System Web Server et Java System Application Server :  
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57498>
- Novell eDirectory :  
<http://support.novell.com/cgi-bin/search/searchtid.cgi?/2967568.htm>
- Check Point :  
Contacter le revendeur.
- Oracle9i database et application server, Oracle HTTP Server :  
<http://otn.oracle.com/deplo/security/pdf/2003alert62.pdf>
- VMWare GSX et ESX Server :  
[http://www.vmware.com/support/kb/enduser/std\\_adp.php?p\\_faqid=1165](http://www.vmware.com/support/kb/enduser/std_adp.php?p_faqid=1165)
- SSH Secure Shell :  
<http://www.ssh.com/company/newsroom/article/476>
- SSH Sentinel :  
<http://www.ssh.com/company/newsroom/article/477>

## 6 Documentation

- Avis de sécurité 006489/TLS du NISCC :  
<http://www.uniras.gov.uk/vuls/2003/006489/tls.htm>
- Avis de sécurité 006489/OpenSSL du NISCC :  
<http://www.uniras.gov.uk/vuls/2003/006489/openssl.htm>
- Avis de sécurité *OpenSSL* :  
[http://www.openssl.org/news/secadv\\_20030930.txt](http://www.openssl.org/news/secadv_20030930.txt)  
[http://www.openssl.org/news/secadv\\_20031104.txt](http://www.openssl.org/news/secadv_20031104.txt)
- Avis de sécurité du CERT/CC du 1er octobre 2003 :  
<http://www.cert.org/advisories/CA-2003-26.html>
- Suivi des vulnérabilités *OpenSSL* du CERT/CC :  
<http://www.kb.cert.org/vuls/id/935264>  
<http://www.kb.cert.org/vuls/id/732952>  
<http://www.kb.cert.org/vuls/id/686224>  
<http://www.kb.cert.org/vuls/id/380864>  
<http://www.kb.cert.org/vuls/id/255484>
- Suivi des vulnérabilités des autres implémentations SSL/TLS du CERT/CC :  
<http://www.kb.cert.org/vuls/id/104280>
- Référence CVE CAN-2003-0543 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0543>
- Référence CVE CAN-2003-0544 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0544>

- Référence CVE CAN-2003-0545 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0545>
- Référence CVE CAN-2003-0851 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0851>

## **Gestion détaillée du document**

**30 septembre 2003** version initiale ;

**1er octobre 2003** correction du lien Cisco, ajout du mauvais respect la spécification de la norme par *OpenSSL*, ajout de Mandrake, Slackware, SGI, *Stunnel*, ajout de nouvelles notes de vulnérabilité du CERT/CC ;

**3 octobre 2003** ajouts de l'avis de sécurité du CERT/CC, d'*Apache* sous HP-UX, de SuSE et Debian ;

**13 octobre 2003** ajouts d'autres produits HP, d'OpenBSD, FreeBSD et NetBSD, mise à jour du lien Apple et introduction de Nortel Networks ;

**16 décembre 2003** Nouvel avis OpenSSL, mise à jour en 0.9.6l, référence CVE CAN-2003-0851, ajouts de Sun, Novell, Check Point, Oracle et VMWare ;

**22 janvier 2004** ajouts des références aux bulletins relatifs à SunPlex (Sun Cluster), Sentinel et Secure Shell de SSH ;

**27 février 2004** ajout d'un nouvel avis NetBSD pour les versions 0.9.6 d'OpenSSL ;

**11 mars 2004** ajout des Java Servers de Sun.