



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 17 juin 2009  
N° CERTA-2009-AVI-120-002

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples 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-2009-AVI-120>

---

### Gestion du document

Référence	CERTA-2009-AVI-120-002
Titre	Multiples vulnérabilités dans OpenSSL
Date de la première version	26 mars 2009
Date de la dernière version	17 juin 2009
Source(s)	Bulletin de sécurité OpenSSL du 25 mars 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

- Déni de service à distance ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

OpenSSL versions antérieures à la 0.9.8k.

## 3 Résumé

Plusieurs vulnérabilités dans OpenSSL permettent à une personne malintentionnée d'effectuer un déni de service à distance ou de contourner la politique de sécurité.

## 4 Description

Plusieurs vulnérabilités ont été découvertes dans OpenSSL :

- une erreur dans la fonction `ASN1_STRING_print_ex()` permet de provoquer un arrêt inopiné de l'application (*crash*) ;

- une vulnérabilité dans la gestion des erreurs permet dans certaines conditions de faire passer une fausse signature pour valide ;
- une erreur dans la gestion des structures *ANSI* mal formées permet de provoquer un arrêt inopiné de l'application (*crash*).

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité OpenSSL du 25 mars 2009 :  
[http://www.openssl.org/news/secadv\\_20090325.txt](http://www.openssl.org/news/secadv_20090325.txt)
- Bulletin de sécurité Debian DSA-1763 du 06 avril 2009 :  
<http://www.debian.org/security/2009/dsa-1763>
- Bulletin de sécurité Gentoo GLSA-200904-08 du 07 avril 2009 :  
<http://www.gentoo.org/security/en/glsa/glsa-200904-08.xml>
- Bulletin de sécurité HP SSRT090059 du 10 juin 2009 :  
[https://www13.itrc.hp.com/service/cki/docDisplay.do?docId=emr\\_na-c017626423](https://www13.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c017626423)
- Bulletin de sécurité Mandriva MDVSA-2009:087 du 03 avril 2009 :  
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:087>
- Bulletin de sécurité OpenSuse SUSE-SR:2009:010 du 12 mai 2009 :  
<http://lists.opensuse.org/opensuse-security-announce/2009-05/msg00000.html>
- Bulletin de sécurité Ubuntu USN-750-1 du 30 mars 2009 :  
<http://www.ubuntu.com/usn/usn-750-1>
- Bulletin de sécurité Sun #258048 du 04 mai 2009 :  
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-258048-1>
- Bulletin de sécurité FreeBSD FreeBSD-SA-09:08.opensll du 22 avril 2009 :  
<http://security.freebsd.org/advisories/FreeBSD-SA-09:08.opensll.asc>
- Bulletin de sécurité OpenBSD #012\_OpenSSL du 08 avril 2009 :  
[http://www.openbsd.org/errata44.html#012\\_openssl](http://www.openbsd.org/errata44.html#012_openssl)
- Bulletin de sécurité OpenBSD #001\_OpenSSL du 08 avril 2009 :  
[http://www.openbsd.org/errata45.html#001\\_openssl](http://www.openbsd.org/errata45.html#001_openssl)
- Référence CVE CVE-2009-0590 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0590>
- Référence CVE CVE-2009-0591 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0591>
- Référence CVE CVE-2009-0789 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0789>

## Gestion détaillée du document

**26 mars 2009** version initiale.

**11 mai 2009** ajout des références aux bulletins de sécurité Gentoo, Debian, Ubuntu, Sun, FreeBSD et OpenBSD.

**17 juin 2009** ajout des références aux bulletins de sécurité Mandriva, HP et Suse.