



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 octobre 2006
N° CERTA-2006-AVI-421

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-2006-AVI-421>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2006-AVI-421 |
| Titre | Multiples Vulnérabilités dans OpenSSL |
| Date de la première version | 03 octobre 2006 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité OpenSSL du 28 septembre 2006 |
| 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 ;
- Exécution de code arbitraire à distance.

2 Systèmes affectés

- OpenSSL versions 0.9.7k et antérieures ;
- OpenSSL versions 0.9.8c et antérieures.

3 Résumé

De multiples vulnérabilités dans OpenSSL permettent à un utilisateur distant de provoquer un déni de service.

4 Description

Trois vulnérabilités sont présentes dans OpenSSL :

- La première vulnérabilité concerne la mise en œuvre du format ASN.1. Elle permet à un utilisateur distant mal intentionné de provoquer un déni de service de l'application utilisant des fonctions de la bibliothèque ASN.1 du OpenSSL vulnérable ;

- La seconde vulnérabilité concerne la fonction `SSL_get_shared_ciphers()`. Elle permet de réaliser un débordement de tampon et potentiellement d'exécuter du code arbitraire ;
- La dernière vulnérabilité concerne la mise en œuvre du protocole `SSLv2` par le client `SSL`. Elle permet de réaliser un déni de service contre le client utilisant la bibliothèque de fonctions `OpenSSL` vulnérable par le biais d'un serveur `OpenSSL` particulier.

5 Solution

Les versions 0.9.7i et 0.9.8d corrigent le problème :
<http://www.openssl.org/source/>

6 Documentation

- Bulletin de sécurité `OpenSSL` du 28 septembre 2006 :
http://www.openssl.org/news/secadv_20060928.txt
- Référence CVE CVE-2006-2937 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2937>
- Référence CVE CVE-2006-2940 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2940>
- Référence CVE CVE-2006-3738 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3738>
- Référence CVE CVE-2006-4343 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4343>

Gestion détaillée du document

03 octobre 2006 version initiale.