Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 octobre 2006
N° CERTA-2006-AVI-448

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités d'OpenSSL sous OpenBSD

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-448

Gestion du document

Référence	CERTA-2006-AVI-448
Titre	Multiples vulnérabilités d'OpenSSL sous OpenBSD
Date de la première version	11 octobre 2006
Date de la dernière version	–
Source(s)	Correctif de sécurité d'OpenBSD du 07 octobre 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

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

2 Systèmes affectés

OpenSSL sous OpenBSD versions 3.8 et 3.9.

3 Description

De multiples vulnérabilités ont été découvertes dans OpenSSL sous OpenBSD. Ces vulnérabilités peuvent être exploitées par un utilisateur mal intentionné afin de provoquer un déni de service et/ou exécuter du code arbitraire à distance sur une machine vulnérable.

4 Solution

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

5 Documentation

- Bulletin de sécurité OpenBSD pour openssl2 du 07 octobre 2006 :
  http://openbsd.org/errata.html#openssl2
- Référence CVE CVE-2006-2937 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2937
- 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
- Référence CVE CVE-2006-2940 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2940

Gestion détaillée du document

11 octobre 2006 version initiale.