Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 mai 2012
N° CERTA-2012-AVI-277

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans OpenSSL

Gestion du document

Référence	CERTA-2012-AVI-277
Titre	Vulnérabilité dans OpenSSL
Date de la première version	15 mai 2012
Date de la dernière version	–
Source(s)	Avis de sécurité OpenSSL 20120210
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.

2 Systèmes affectés

Les applications DTLS reposant sur les versions vulnérables de OpenSSL (client ou serveur) sont vulnérables. Les versions antérieures à 1.0.1c, 1.0.0j et 0.9.8x sont vulnérables.

3 Résumé

Une vulnérabilité dans la gestion des *ciphersuites* en mode CBC a été corrigée dans OpenSSL. Cette vulnérabilité peut-être exploitée pour provoquer un déni de service dans les applications liées à la librairie OpenSSL pour implémenter le protocole DTLS. Seul OpenSSL 1.0.1 et supérieur expose également le protocole TLS.

4 Solution

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

5 Documentation

- Référence CVE CVE-2012-2333 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2333
- Référence Avis OpenSSL 20120510 :
  http://www.openssl.org/news/secadv_20120510.txt

Gestion détaillée du document

15 mai 2012 version initiale.