Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 mars 2012
N° CERTA-2012-AVI-134

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans OpenSSL

Dernière version de ce document : http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-134

Gestion du document

Référence	CERTA-2012-AVI-134
Titre	Vulnérabilités dans OpenSSL
Date de la première version	13 mars 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité OpenSSL du 12 mars 2012
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 1.0.0g et antérieures ;
- OpenSSL versions 0.9.8t et antérieures.

3 Résumé

Des vulnérabilités ont été corrigées dans OpenSSL et permettent de provoquer un déni de service à distance.

4 Description

Deux vulnérabilités ont été corrigées dans OpenSSL. Elles permettent à un attaquant de contourner la politique de sécurité et de provoquer un déni de service à distance.

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 12 mars 2012 :
  http://www.openssl.org/news/secadv_20120312.txt
- Référence CVE CVE-2012-0884 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0884
- Référence CVE CVE-2012-1165 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1165

Gestion détaillée du document

13 mars 2012 version initiale.