Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 février 2013
N° CERTA-2013-AVI-099

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans OpenSSL

Gestion du document

Référence	CERTA-2013-AVI-099
Titre	Multiples vulnérabilités dans OpenSSL
Date de la première version	07 février 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité du 05 février 2013
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(s)

- déni de service à distance
- atteinte à la confidentialité des données

2 Systèmes affectés

- OpenSSL version 1.0.1c
- OpenSSL version 1.0.0j
- OpenSSL version 0.9.8x

3 Résumé

De multiples vulnérabilités ont été corrigées dans *OpenSSL*. Elles permettent à un attaquant de provoquer un déni de service à distance et une atteinte à la confidentialité des données.

4 Solution

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

5 Documentation

- Bulletin de sécurité OpenSSL du 05 février 2013
  http://www.openssl.org/news/secadv_20130204.txt
- Référence CVE CVE-2012-2686
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2686
- Référence CVE CVE-2013-0166
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0166
- Référence CVE CVE-2013-0169
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0169

Gestion détaillée du document

07 février 2013 version initiale.