



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 septembre 2011
N° CERTA-2011-AVI-496

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-2011-AVI-496>

Gestion du document

Référence	CERTA-2011-AVI-496-001
Titre	Vulnérabilités dans OpenSSL
Date de la première version	07 septembre 2011
Date de la dernière version	16 septembre 2011
Source(s)	Bulletin de sécurité OpenSSL du 06 septembre 2011
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 version 1.0.0d et antérieures ;
- OpenSSL versions 0.9.8 à 0.9.8s (experimental « ECCdraft » ciphersuite).

3 Résumé

Deux vulnérabilités dans OpenSSL permettent à une personne malintentionnée de contourner la politique de sécurité ou de provoquer un déni de service à distance.

4 Description

Deux vulnérabilités ont été découvertes dans OpenSSL :

- une vulnérabilité dans le processus de vérification de certificats internes au serveur permet la validation

d'une liste de révocation de certificats incorrecte. Cette vulnérabilité n'est présente que dans la branche 1.x d'OpenSSL (CVE-2011-3207) ;

- une erreur dans la gestion des messages de négociation de session d'*OpenSSL server code for ephemeral ECDH ciphersuite* permet à une personne distante malintentionnée de provoquer un déni de service (CVE-2011-3210).

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 06 septembre 2011 :
http://www.openssl.org/news/secadv_20110906.txt
- Bulletin de sécurité Fedora FEDORA-2011-12281 du 10 septembre 2011 :
<http://lists.fedoraproject.org/pipermail/package-announce/2011-September/065712.html>
- Référence CVE CVE-2011-3207 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3207>
- Référence CVE CVE-2011-3210 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3210>

Gestion détaillée du document

07 septembre 2011 version initiale.

16 septembre 2011 ajout d'une référence au bulletin Fedora.