



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 mai 2011
N° CERTA-2010-AVI-590-002

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-2010-AVI-590>

Gestion du document

Référence	CERTA-2010-AVI-590-002
Titre	Vulnérabilités dans OpenSSL
Date de la première version	14 décembre 2010
Date de la dernière version	04 mai 2011
Source(s)	Bulletin de sécurité OpenSSL du 02 décembre 2010
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

Contournement de la politique de sécurité.

2 Systèmes affectés

- versions inférieures à 0.9.8q et 1.0.x avant 1.0.0c (CVE-2010-4180) ;
- versions inférieures à 1.0.0c (CVE-2010-4252) ;

3 Résumé

Deux vulnérabilités ont été corrigées dans OpenSSL. Elles permettent à un utilisateur de contourner la politique de sécurité.

4 Description

La première vulnérabilité corrigée (CVE-2010-4180) permet à un utilisateur malveillant de forcer les connexions futures à utiliser un algorithme de chiffrement faible.

La seconde (CVE-2010-4252) permet à un utilisateur malveillant de s'authentifier sans connaître le secret partagé lorsque le protocole J-PAKE est utilisé.

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 02 décembre 2010 :
http://www.openssl.org/news/secadv_20101202.txt
- Bulletin de sécurité HP HPSBUS02638 SSRT100339 du 03 mars 2011 :
http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02737002
- Bulletin de sécurité Oracle Solaris du 29 avril 2011 :
http://blogs.sun.com/security/entry/cve_2010_4180_affects_openssl
- Référence CVE CVE-2010-4180 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4180>
- Référence CVE CVE-2010-4252 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4252>

Gestion détaillée du document

14 décembre 2010 version initiale.

04 mars 2011 Ajout de la référence au bulletin de sécurité HP-UX.

04 mai 2011 Ajout de la référence au bulletin de sécurité Oracle Solaris.