



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 décembre 2010
N° CERTA-2010-AVI-237-001

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-237>

Gestion du document

Référence	CERTA-2010-AVI-237-001
Titre	Vulnérabilités dans OpenSSL
Date de la première version	04 juin 2010
Date de la dernière version	03 décembre 2010
Source(s)	Bulletin de sécurité OpenSSL du 01 juin 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

- Exécution de code arbitraire à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- OpenSSL versions antérieures à la 0.9.8o ;
- OpenSSL versions antérieures à la 1.0.0a.

3 Résumé

Deux vulnérabilités ont été découvertes dans OpenSSL et permettent à une personne malintentionnée de contourner la politique de sécurité ou d'exécuter du code arbitraire à distance.

4 Description

Deux vulnérabilités ont été découvertes dans OpenSSL :

- une erreur dans la gestion des données *OriginatorInfo* de la structure CMS permet à une personne malintentionnée d'exécuter du code arbitraire à distance (CVE-2010-0742) ;
- une erreur dans la fonction *EVP_PKEY_verify_recover()* permet à une personne malintentionnée de contourner le système de vérification des clés (CVE-2010-1633).

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 01 juin 2010 :
http://www.openssl.org/news/secadv_20100601.txt
- Bulletin de sécurité HP c2629503 du 01 décembre 2010 :
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c2629503>
http://www13.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c2629503
- Référence CVE CVE-2010-0742 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0742>
- Référence CVE CVE-2010-1633 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1633>

Gestion détaillée du document

04 juin 2010 version initiale.

03 décembre 2010 ajout de la référence au bulletin HP.