Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 mai 2012
N° CERTA-2012-AVI-224-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans OpenSSL

Gestion du document

Référence	CERTA-2012-AVI-224-001
Titre	Vulnérabilité dans OpenSSL
Date de la première version	20 avril 2012
Date de la dernière version	09 mai 2012
Source(s)	Bulletin de sécurité OpenSSL du 19 avril 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Versions antérieures à OpenSSL 1.0.1a ;
- versions antérieures à OpenSSL 1.0.0i ;
- versions antérieures à OpenSSL 0.9.8v.

3 Résumé

Une vulnérabilité a été corrigée dans *OpenSSL*. Elle affecte la fonction « asn1_d2i_read_bio » qui n'est pas obligatoirement utilisée lors des communications SSL/TLS. Toutes les applications basées sur les fonctions BIO ou FILE pour lire un format DER non fiable sont vulnérables.

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 19 avril 2012 :
  http://www.openssl.org/news/secadv_20120419.txt
- Bulletin de sécurité IBM OS/400 SE51936 du 08 mai 2012 :
  http://www-01.ibm.com/support/docview.wss?uid=nas2d7439844d1fd14f0862579f5003c71ce
- Référence CVE CVE-2012-2110 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2110

Gestion détaillée du document

20 avril 2012 version initiale ;
09 mai 2012 ajout du bulletin IBM OS/400.