Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 février 2012
N° CERTA-2010-AVI-555-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans OpenSSL

Gestion du document

Référence	CERTA-2010-AVI-555-003
Titre	Vulnérabilité dans OpenSSL
Date de la première version	17 novembre 2010
Date de la dernière version	06 février 2012
Source(s)	Bulletin de sécurité OpenSSL du 16 novembre 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 ;
- déni de service à distance.

2 Systèmes affectés

Toutes les versions de OpenSSL implémentant les extensions TLS. Ceci inclut :
- OpenSSL versions 0.9.8f à 0.9.8o ;
- OpenSSL versions 1.0.0 et 1.0.0a.

3 Résumé

Une vulnérabilité présente dans OpenSSL permet à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Une vulnérabilité est présente dans `OpenSSL`. Elle est relative à la gestion de la mise en cache interne. Ainsi seules sont vulnérables les applications mettant en œuvre du *multi-threading* et s'appuyant sur la mise en cache interne de `OpenSSL`. L'exploitation de cette faille permet à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire.

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 16 novembre 2010 :
  http://www.openssl.org/news/secadv_20101116.txt
- Bulletin de sécurité FreeBSD FreeBSD-SA-10:10 du 29 novembre 2010 :
  http://security.freebsd.org/advisories/FreeBSD-SA-10:10.openssl.asc
- Bulletin de sécurité Debian DSA-2125 du 22 novembre 2010 :
  http://www.debian.org/security/2010/dsa-2125
- Bulletin de sécurité HP du HPSBUS02638 SSRT100339 du 03 mars 2011 :
  http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02737002
- Bulletin de sécurité HP c03179825 du 02 février 2012 :
  http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03179825
- Référence CVE CVE-2010-3864 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3864

Gestion détaillée du document

17 novembre 2010 version initiale.
02 décembre 2010 ajout des références aux bulletins de sécurité FreeBSD et Debian.
04 mars 2011 Ajout de la référence au bulletin de sécurité HP-UX.
06 février 2012 Ajout de la référence au bulletin de sécurité HP.