Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 septembre 2006
N° CERTA-2006-AVI-384-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans OpenSSL

Gestion du document

Référence	CERTA-2006-AVI-384-002
Titre	Vulnérabilité dans OpenSSL
Date de la première version	06 septembre 2006
Date de la dernière version	11 septembre 2006
Source(s)	Bulletin de sécurité OpenSSL du 05 septembre 2006
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

Les versions d'OpenSSL antérieures à 0.9.7k et 0.9.8c.

3 Description

Une vulnérabilité a été identifiée dans OpenSSL. Elle permettrait à une personne malveillante de construire une signature PKCS #1 v1.5 à partir d'une clé RSA utilisant un exposant 3. La vérification de la clef ne serait pas effectuée de manière correcte par OpenSSL au moment de la signature.

Une manière usuelle de créer ce genre de clé nécessite la commande suivante : *openssl genrsa -3 taille_clé | tee ma_signature.PEM*. La signature s'obtient par la commande `openssl rsautl -sign`.

4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Référence CVE CVE-2006-4339 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4339
- Annonce OpenSSL du 05 Septembre 2006 :
  http://www.openssl.org/news/secadv_20060905.txt
- Site pour le téléchargement des dernières mises à jour OpenSSL :
  http://www.openssl.org/source/
- Mise à jour Ubuntu USN-339-1 du 05 septembre 2006 :
  http://www.ubuntu.com/usn/usn-339-1
- Mise à jour FreeBSD SA-06:19.openssl du 06 septembre 2006 :
  http://security.freebsd.org/advisories/FreeBSD-SA-06:19.openssl.asc
- Mise à jour Mandriva MDKSA-2006:161 du 06 septembre 2006 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2006:161
- Mise à jour Redhat RHSA-2006:0661-8 du 06 septembre 2006 :
  http://rhn.redhat.com/errata/RHSA-2006-0661.html
- Mise à jour Gentoo GLSA-200609-05 du 07 septembre 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200609-05.xml
- Bulletin de sécurité Debian DSA-1173 du 09 septembre 2006 :
  http://www.debian.org/security/2006/dsa-1173
- Bulletin de sécurité OpenBSD du 08 septembre 2006 :
  http://www.openbsd.org/errata.html

Gestion détaillée du document

06 septembre 2006 version initiale.
08 septembre 2006 ajout des références aux mises à jour FreeBSD, Mandriva, Gentoo et Redhat.
11 septembre 2006 ajout de la référence aux bulletins de sécurité Debian et OpenBSD.