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 janvier 2006
N° CERTA-2005-AVI-400-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Faiblesse dans OpenSSL 0.9.x

Gestion du document

Référence	CERTA-2005-AVI-400-004
Titre	Faiblesse dans OpenSSL 0.9.x
Date de la première version	12 octobre 2005
Date de la dernière version	04 janvier 2006
Source(s)	Avis OpenSSL du 11 octobre 2005
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,
- risque d'atteinte à la confidentialité des échanges.

2 Systèmes affectés

Tout système utilisant *OpenSSL* en versions sources 0.9.7 jusqu'à 0.9.7g ou 0.9.8 et les betas antérieures.

Par extension, sont concernés tous les serveurs utilisant *OpenSSL* pour le support de SSL/TLS. En particulier les versions SSL du serveur web *Apache*, des serveurs de courrier *qmail*, *postfix*, *Exim*, du serveur d'annuaire *OpenLDAP*,. . . peuvent être impactés.

3 Résumé

Un utilisateur mal intentionné, ayant la capacité d'intercepter le flux TCP, peut conduire une attaque par le milieu visant à faire régresser à la version 2 le protocole SSL négocié entre les parties.

4 Description

OpenSSL est une mise en oeuvre « open source » des protocoles Secure Sockets Layer (SSL) et Transport Layer Security (TLS). *OpenSSL* est largement utilisé comme bibliothèque pour sécuriser des protocoles applicatifs sur l'Internet.

Les versions du protocole SSL usuellement supportée sont v2 et v3, sachant que l'on peut assimiler TLS à une version v3.1. Cependant le support de v2 n'est conservé que pour des raisons de compatibilité ascendante et n'est plus vraiment justifié de nos jours la v3 datant de novembre 1996. L'usage de SSLv2 est fortement déconseillé étant donné des faiblesses cryptographiques majeures qui ont conduit à l'élaboration de la version v3.

L'usage d'un code, développé pour assurer la compatibilité avec des produits tiers, supprime la vérification d'une éventuelle attaque en régression sur la version négociée, lors de l'établissement d'une session SSLv2.

Il est ainsi possible, pour un utilisateur en position d'interception, de forcer l'utilisation de SSLv2 entre 2 parties alors que SSLv3 ou TLS étaient possibles. Celui-ci pourra alors tenter d'exploiter les faiblesses de SSLv2 pour attenter à la confidentialité de l'échange.

5 Contournement provisoire

Désactiver le support de SSLv2 dans toute application utilisant *OpenSSL*.

6 Solution

Mettre à jour les sources en versions 0.9.7h ou 0.9.8a au moins, ou se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Site internet d'*OpenSSL* :
  http://www.openssl.org
- Avis de sécurité *OpenSSL* du 11 octobre 2005 :
  http://www.openssl.org/news/secadv_20051011.txt
- Bulletin de sécurité RedHat RHSA-2005:800 du 11 octobre 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-800.html
- Bulletin de sécurité Gentoo GLSA-200510-11 du 12 octobre 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200510-11.xml
- Bulletin de sécurité Mandriva MDKSA-2005:179 du 11 octobre 2005 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2005:179
- Bulletin de sécurité SUSE SuSE-SA:2005:061 du 19 octobre 2005 :
  http://www.novell.com/linux/security/advisories/2005_61_openssl.html
- Linux Fedora :
  - Fedora Core 3 du 31 octobre 2005 :
    http://marc.theaimsgroup.com/?l=fedora-announce-list&m=11307879729070
  - Fedora Core 4 du 13 octobre 2005 :
    http://marc.theaimsgroup.com/?l=fedora-announce-list&m=112931336325090
- Debian GNU/Linux :
  - Bulletin de sécurité Debian DSA 875 du 27 octobre 2005 pour *OpenSSL* 0.9.4 :
    http://www.debian.org/security/2005/dsa-875
  - Bulletin de sécurité Debian DSA 881 du 04 novembre 2005 pour *OpenSSL* 0.9.6 :
    http://www.debian.org/security/2005/dsa-881
  - Bulletin de sécurité Debian DSA 882 du 04 novembre 2005 pour *OpenSSL* 0.9.5 :
    http://www.debian.org/security/2005/dsa-882
  - Bulletin de sécurité Debian DSA 888 du 07 novembre 2005 pour *OpenSSL* :
    http://www.debian.org/security/2005/dsa-888
- Bulletin de sécurité Ubuntu USN-204 du 14 octobre 2005 :
  http://www.ubuntu.com/usn/usn-204-1

- Bulletin de sécurité FreeBSD SA-05-21 du 11 octobre 2005 :
  ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05-21.openssl.asc
- Bulletin de sécurité Sun #101974 du 11 octobre 2005 pour Solaris 10 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-26-101974-1
- Bulletin de sécurité Cisco du 02 décembre 2005 :
  http://www.cisco.com/warp/public/707/cisco-response-20051202-openssl.shtml
- Bulletin de sécurité Juniper du 08 décembre 2005 :
  http://www.juniper.net/support/security/alerts/PSN-2005-12-025.txt
- Référence CVE CAN-2005-2969 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2969

Gestion détaillée du document

12 octobre 2005 version initiale ;
07 novembre 2005 ajouts des bulletins Fedora Core 3 et 4, du bulletin SuSE et de 3 avis Debian ;
08 novembre 2005 ajout des références aux bulletins de sécurité Debian DSA-888 et Ubuntu ;
05 décembre 2005 ajout de la référence à l'avis de sécurité Cisco.
04 janvier 2006 ajout de la référence à l'avis de sécurité Juniper.