Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 septembre 2002
N° CERTA-2002-AVI-162-006

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans OpenSSL

Gestion du document

Référence	CERTA-2002-AVI-162-006
Titre	Multiples vulnérabilités dans OpenSSL
Date de la première version	31 juillet 2002
Date de la dernière version	26 septembre 2002
Source(s)	Avis CA-2002-23 du CERT/CC
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 ;
- déni de service.

2 Systèmes affectés

Tout système possédant les versions `0.9.6d` et antérieures, les versions `0.9.7-beta2` et antérieures (y compris les versions en développement collectées sur le CVS) de `OpenSSL` est vulnérable. Un système 32 bits possédant la version `0.9.6d` sur laquelle `SSL 2.0` est désactivé n'est pas vulnérable.

De nombreux produits incluent `OpenSSL` en standard et sont donc tout autant vulnérables (Consultez la section Documentation).

3 Résumé

Plusieurs vulnérabilités de type débordement de mémoire permettent à un utilisateur mal intentionné de provoquer l'exécution de code arbitraire ou un déni de service.

4 Description

OpenSSL est une librairie de fonctions créée pour implémenter les protocoles SSL (Secure Sockets Layer), TLS (Transport Layer Security) ainsi que de nombreux utilitaires de cryptographie. Plusieurs vulnérabilités ont été découvertes permettant à un utilisateur mal intentionné d'exécuter du code arbitraire ou de provoquer un déni de service.

5 Contournement provisoire

Désactiver le support de `SSL 2.0`, désactiver les applications utilisant `SSL` ou `TLS` en attendant que le correctif soit appliqué. Les utilisateurs des versions de développement `pré-0.9.7` utilisant `Kerberos` doivent aussi désactiver `Kerberos`.

6 Solution

Téléchargez le ou les correctifs correspondants à la version d'OpenSSL installée sur votre système (cf. section documentation)

7 Documentation

- Avis #CA-2002-23 du CERT CC
  http://www.cert.org/advisories/CA-2002-23.html
- Le site d'OpenSSL :
  http://www.openssl.org/
- Le site du module SSL du serveur WEB Apache :
  http://www.apache-ssl.org/
- Bulletin de sécurité #RHSA-2002:160-21 de RedHat :
  http://rhn.redhat.com/errata/RHSA-2002-160.html
- Bulletin de sécurité #DSA-136-2 Debian :
  http://www.debian.org/security/2002/dsa-136
- Bulletin de sécurité #SuSE-SA:2002:027 de SuSE :
  http://www.suse.com/de/security/2002_027_openssl.html
- Bulletin de sécurité #MDKSA-2002:046 de Mandrake :
  http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-046.php
- Bulletin de sécurité #NETBSD-SA2002-009 de NetBSD :
  ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2002-009.txt.asc
- Bulletin de sécurité 2002-08-02 de apple :
  http://www.info.apple.com/usen/security/security_updates.html
- Bulletin de sécurité #46424 de SUN :
  http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F46424
- Bulletin de sécurité #46605 de SUN :
  http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F46605
- Bulletin de sécurité #37 d'Oracle :
  http://technet.oracle.com/deploy/security/pdf/openssl/Alert.pdf
- Bulletin de sécurité de #SSRT2310a de Hewlett Packard/Compaq
  http://thenew.hp.com/country/fr/fre/support.html

Gestion détaillée du document

31 juillet 2002 version initiale ;
05 août 2002 ajout des bulletins de Mandrake, NetBSD et apple ;
20 août 2002 ajout du bulletin #46424 de SUN ;
21 août 2002 ajout de l'avis Oracle et modification de l'avis RedHat ;

04 septembre 2002 ajout de l'avis HP/Compaq ;
17 septembre 2002 M.A.J. de l'avis Debian, ajout de l'avis du CERT CC ;
26 septembre 2002 ajout de l'avis #46605 de SUN.