



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 7 mars 2003
N° CERTA-2003-AVI-029-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans SSL/TLS

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-029>

Gestion du document

Référence	CERTA-2003-AVI-029-002
Titre	Vulnérabilité dans SSL/TLS
Date de la première version	21 février 2003
Date de la dernière version	7 mars 2003
Source(s)	Bulletin OpenSSL
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

Atteinte à la confidentialité des données.

2 Systèmes affectés

OpenSSL versions antérieures à 0.9.6i et 0.9.7a.

3 Résumé

Une vulnérabilité présente dans certaines implémentations du protocole SSL/TLS permet à un utilisateur mal intentionné de retrouver le clair d'un contenu chiffré.

4 Description

Lors d'une session SSL/TLS utilisant le mode de chiffrement CBC (Cipher Block Chaining) les temps de réponses du serveur peuvent différer suivant le type d'erreur rencontré.

Un utilisateur mal intentionné peut, sous certaines conditions, reconstituer un même bloc de données transitant dans plusieurs sessions chiffrées en injectant des paquets judicieusement composés et en mesurant le temps de traitement de ces paquets.

Cette attaque peut permettre, par exemple, d'identifier un mot de passe dans une session SSL/TLS.

5 Solution

Appliquer le correctif fourni par l'éditeur (Cf. section Documentation)

6 Documentation

- Avis de sécurité OpenSSL :
http://www.openssl.org/news/secadv_20030219.txt
- Bulletin de sécurité DSA-253 de Debian :
<http://www.debian.org/security/2003/dsa-253>
- Bulletin de sécurité MDKSA-2003:020 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:020>
- Bulletin de sécurité SuSE-SA:2003:011 de SuSE :
http://www.suse.com/de/security/2003_011_openssl.html
- Bulletin de sécurité FreeBSD-SA-03:02.openssl de FreeBSD :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-03:02.openssl.asc>
- Bulletin de sécurité d'OpenBSD du 22 février 2003 :
<http://www.openbsd.org/errata.html#ssl>
- Bulletin de sécurité 2003-001 de NetBSD :
<http://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-001.txt.asc>
- Mise à jour pour Mac OS X du 2003-03-03 :
<http://docs.info.apple.com/article.html?artnum=61798>
- Bulletin de sécurité RHSA-2003-062 de Red Hat :
<http://rhn.redhat.com/errata/RHSA-2003-062.html>

Gestion détaillée du document

21 février 2003 version initiale.

27 février 2003 ajout références aux bulletins de Debian, Mandrake, SuSE, OpenBSD, FreeBSD.

7 mars 2003 ajout références aux bulletins de NetBSD, Apple et Red Hat.