Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 juin 2009
N° CERTA-2008-AVI-556-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans GnuTLS

Gestion du document

Référence	CERTA-2008-AVI-556-002
Titre	Vulnérabilité dans GnuTLS
Date de la première version	14 novembre 2008
Date de la dernière version	17 juin 2009
Source(s)	Bulletin de mise à jour 2.6.2 du 12 novembre 2008
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

- Déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Les versions de *GnuTLS* antérieures à la 2.6.2.

3 Résumé

Une vulnérabilité dans le traitement des certificats X.509 a été corrigée.

4 Description

Une vulnérabilité dans le traitement des certificats X.509 permettant d'utiliser un nom arbitraire a été corrigée dans la version 2.6.1. Cette dernière a été remplacée par la 2.6.2 car elle souffrait d'un défaut lors du traitement des certificats auto-signés qui provoquait des arrêts inopinés.

5 Solution

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

6 Documentation

- Détails de la mise à jour 2.6.2 de GnuTLS :
  http://article.gmane.org/gmane.comp.encryption.gpg.gnutls.devel/3248
- Bulletin de sécurité Debian DSA-1719 du 10 février 2009 :
  http://www.debian.org/security/2009/dsa-1719
- Bulletin de sécurité Fedora FEDORA-2008-9530 du 12 novembre 2008 :
  https://www.redhat.com/archives/fedora-package-announce/2008-November/msg00222.html
- Bulletin de sécurité Fedora FEDORA-2008-9600 du 12 novembre 2008 :
  https://www.redhat.com/archives/fedora-package-announce/2008-November/msg00293.html
- Bulletin de sécurité Gentoo GLSA-200901-10 du 14 janvier 2009 :
  http://www.gentoo.org/security/en/glsa/glsa-200901-10.xml
- Bulletin de sécurité Red Hat RHSA-2008:0982 du 11 novembre 2008 :
  http://rhn.redhat.com/errata/RHSA-2008-0982.html
- Bulletin de sécurité Sun 260528 du 10 juin 2009 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-66-260528-1
- Bulletin de sécurité SuSE SuSE-SR:2008:027 du 09 décembre 2008 :
  http://lists.opensuse.org/opensuse-security-announce/2008-12/msg00002.html
- Bulletin de sécurité Ubuntu USN-678-1 du 26 novembre 2008 :
  http://www.ubuntu.com/usn/usn-678-1
- Bulletin de sécurité Ubuntu USN-678-2 du 10 décembre 2008 :
  http://www.ubuntu.com/usn/usn-678-2
- Référence CVE CVE-2008-4989 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4989

Gestion détaillée du document

14 novembre 2008 version initiale.
06 mars 2009 ajout des références aux bulletins de sécurité Gentoo, Debian, Red Hat, SuSE et Ubuntu.
17 juin 2009 ajout des références aux bulletins de sécurité Fedora et Sun.