Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 août 2009
N° CERTA-2009-AVI-336-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans GnuTLS

Gestion du document

Référence	CERTA-2009-AVI-336-001
Titre	Vulnérabilité dans GnuTLS
Date de la première version	13 août 2009
Date de la dernière version	21 août 2009
Source(s)	Bulletin de sécurité GNUTLS-SA-2009-4 du 10 août 2009
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

GnuTLS, version 2.8.1 et versions antérieures.

3 Résumé

Une vulnérabilité dans GnuTLS permet à un utilisateur malveillant de contourner la politique de sécurité.

4 Description

Un défaut de traitement d'un certificat de clef publique dont le champ *commonName* ou le champ *subjectAlternateName* contient un caractère ASCII *null* conduit à un affichage inexact de ces champs ou à une absence de détection de différence avec un nom d'hôte. Ce défaut peut être exploité par un utilisateur malveillant pour tromper l'utilisateur sur l'identité d'un serveur sur lequel il est connecté.

5 Solution

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

6 Documentation

- Site de téléchargement du projet GnuTLS :
  http://www.gnu.org/software/gnutls/download.html
- Bulletin de sécurité GNUTLS-SA-2009-4 du 10 août 2009 :
  http://www.gnu.org/software/gnutls/security.html
- Bulletin de sécurité Ubuntu USN-809-1 du 19 août 2009 :
  http://www.ubuntu.com/usn/usn-809-1
- Référence CVE CVE-2009-2730 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2730

Gestion détaillée du document

13 août 2009 version initiale.
21 août 2009 ajout de la référence au bulletin de sécurité Ubuntu.