Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 février 2013
N° CERTA-2013-AVI-109

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans GnuTLS

Gestion du document

Référence	CERTA-2013-AVI-109
Titre	Vulnérabilité dans GnuTLS
Date de la première version	08 février 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité GnuTLS du 04 février 2013
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(s)

– atteinte à la confidentialité des données

2 Systèmes affectés

– GnuTLS versions antérieures à 3.1.7
– GnuTLS versions antérieures à 3.0.28
– GnuTLS versions antérieures à 2.12.23

3 Résumé

Une vulnérabilité a été corrigée dans *GnuTLS* . Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. Il s'agit de l'attaque présentée dans *Lucky Thirteen: Breaking the TLS and DTLS Record Protocols*

4 Solution

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

5 Documentation

- Bulletin de sécurité GnuTLS du 04 février 2013
  http://www.gnutls.org/security.html
- Référence CVE CVE-2013-1619
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1619

Gestion détaillée du document

08 février 2013 version initiale.