Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 mars 2012
N° CERTA-2012-AVI-167

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans GnuTLS

Gestion du document

Référence	CERTA-2012-AVI-167
Titre	Vulnérabilités dans GnuTLS
Date de la première version	22 mars 2012
Date de la dernière version	–
Source(s)	Avis de sécurité GNUTLS-SA-2012-2 et GNUTLS-SA-2012-3
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.

2 Systèmes affectés

- Versions vulnérables à CVE-2012-1569 :
  - GnuTLS 2.x versions inférieures à 2.12.17 ;
  - GnuTLS 3.x versions inférieures à 3.0.15.
- Versions vulnérables à CVE-2012-1573 :
  - GnuTLS versions 2.x versions inférieures à 2.12.18 ;
  - GnuTLS versions 3.x versions inférieures à 3.0.16.

3 Résumé

Deux vulnérablités permettant à un attaquant distant de réaliser un déni de service à distance ont été corrigées dans *GnuTLS*.

4 Description

Une première vulnérabilité affectant la bibliothèque *libtasn1* (incluse dans *GnuTLS*) a été corrigée (CVE-2012-1569). Elle permet à un attaquant de réaliser un déni de service à distance.

Une deuxième vulnérabilité dans l'analyse d'enregistrements TLS permet à un attaquant de réaliser un déni de service à distance au moyen d'une structure `GenericBlockCipher` spécialement conçue.

5 Solution

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

6 Documentation

- Avis de sécurité GNUTLS-SA-2012-2 et GNUTLS-SA-2012-3 :
  http://www.gnu.org/software/gnutls/security.html
- Référence CVE CVE-2012-1573 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1573
- Référence CVE CVE-2012-1569 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1569

Gestion détaillée du document

22 mars 2012 version initiale.