Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 août 2008
N° CERTA-2008-AVI-424

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans GnuTLS

Gestion du document

Référence	CERTA-2008-AVI-424
Titre	Vulnérabilité dans GnuTLS
Date de la première version	20 août 2008
Date de la dernière version	–
Source(s)	Annonce CVE-2008-2377 du 12 août 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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

- Les versions de GnuTLS antérieures à 2.4.1.

3 Résumé

Une vulnérabilité a été identifiée dans la bibliothèque GnuTLS. L'exploitation de cette dernière permettrait sous certaines conditions à une personne distante de perturber voire d'exécuter du code arbitraire sur le système vulnérable.

4 Description

Une vulnérabilité a été identifiée dans la bibliothèque GnuTLS. Elle concerne la fonction `_gnutls_handshake_hash_buff` qui ne manipulerait pas correctement certaines données.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Il faut noter que la nouvelle branche de GnuTLS (2.5.x) est en cours de développement depuis le début du mois de juillet. Les dernières modifications ont été effectuées dans la version 2.5.4.

Cependant, à la date de rédaction de cet avis, la dernière version stable est la 2.4.1.

6 Documentation

- Répertoires de téléchargement de la bibliothèque GnuTLS :
  ftp://ftp.gnutls.org/pub/gnutls/
- Détails du correctif appliqué dans la branche 2.4.1 :
  http://article.gmane.org/gmane.comp.encryption.gpg.gnutls.devel/2947
- Annonces de sécurité GnuTLS :
  http://www.gnu.org/software/gnutls/security.html
- Référence CVE CVE-2008-2377 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2377

Gestion détaillée du document

20 août 2008 version initiale.