

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans GnuTLS

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-632>

Gestion du document

Référence	CERTA-2011-AVI-632
Titre	Vulnérabilité dans GnuTLS
Date de la première version	14 novembre 2011
Date de la dernière version	–
Source	Annonce de publication des versions 3.0.7 et 2.12.14 de GnuTLS 10 novembre 2011
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

GnuTLS 3.x et 2.x.

3 Résumé

Une vulnérabilité dans GnuTLS permet à un utilisateur malveillant de provoquer un déni de service à distance.

4 Description

Dans certaines formes d'appel à la fonction `gnutls_session_get_data` de GnuTLS, il est possible de provoquer un débordement de zone mémoire. Cette exploitation provoque au minimum un déni de service à distance.

5 Solution

Les versions 3.0.7 et 2.12.14 de GnuTLS corrigent ces vulnérabilités.

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

6 Documentation

- Annonce de publication des versions 3.0.7 et 2.12.14 de GnuTLS 10 novembre 2011 :
<http://www.gnu.org/software/gnutls/security.html>
- Référence CVE CVE-2011-4128 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4128>

Gestion détaillée du document

14 novembre 2011 version initiale.