

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

### Objet : Vulnérabilité dans GnuTLS

### Gestion du document

Référence	CERTFR-2014-AVI-097
Titre	Vulnérabilité dans GnuTLS
Date de la première version	03 mars 2014
Date de la dernière version	–
Source(s)	Bulletin de sécurité GnuTLS GNUTLS-SA-2014-2 du 03 mars 2014
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)

- contournement de la politique de sécurité
- atteinte à la confidentialité des données

### 2 - Systèmes affectés

- Versions antérieures à GnuTLS 3.2.12
- versions antérieures à GnuTLS 3.1.22

### 3 - Résumé

Une vulnérabilité a été corrigée dans *GnuTLS*. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité et une atteinte à la confidentialité des données.

### 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 GNUTLS-SA-2014-2 du 03 mars 2014  
<http://gnutls.org/security.html#GNUTLS-SA-2014-2>
- Référence CVE CVE-2014-0092  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0092>

## Gestion détaillée du document

**03 mars 2014** version initiale.

---

Conditions d'utilisation de ce document : <http://cert.ssi.gouv.fr/cert-fr/apropos.html>  
Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2014-AVI-097>

---