

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

### Objet : Vulnérabilité dans GnuTLS

### Gestion du document

Référence	CERTFR-2015-AVI-180
Titre	Vulnérabilité dans GnuTLS
Date de la première version	16 avril 2015
Date de la dernière version	–
Source(s)	Bulletin de sécurité GnuTLS GNUTLS-SA-2015-1 du 30 mars 2015
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

### 2 - Systèmes affectés

GnuTLS versions antérieures à 3.1.0

### 3 - Résumé

Une vulnérabilité a été corrigée dans *GnuTLS*. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité.

### 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-2015-1 du 30 mars 2015  
<http://gnutls.org/security.html#GNUTLS-SA-2015-1>

– Référence CVE CVE-2015-0282  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0282>

## **Gestion détaillée du document**

**16 avril 2015** 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-2015-AVI-180>

---