



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 18 septembre 2008  
N° CERTA-2008-AVI-262-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités 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-2008-AVI-262>

---

### Gestion du document

Référence	CERTA-2008-AVI-262-001
Titre	Multiples vulnérabilités dans GnuTLS
Date de la première version	22 mai 2008
Date de la dernière version	18 septembre 2008
Source(s)	Note de version GnuTLS du 19 mai 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

- GnuTLS 1.x ;
- GnuTLS 2.x ;
- FileZilla 2.x ;
- FileZilla 3.x.

## 3 Résumé

De multiples vulnérabilités ont été découvertes dans *GnuTLS* et permettent à une personne malveillante d'effectuer un déni de service ou une exécution de code arbitraire à distance.

## 4 Description

Plusieurs vulnérabilités de *GnuTLS* permettent à une personne malveillante d'effectuer un déni de service ou une exécution de code à distance. Ces vulnérabilités peuvent être exploitées via :

- des messages *Client Hello* dans des packets *TLS* spécialement conçus ;
- des données *TLS* chiffrées spécialement conçues exploitant une erreur dans la fonction `_gnutls_ciphertext2compressed()`.

## 5 Solution

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

## 6 Documentation

- Note de version GnuTLS 2.2.5 du 19 mai 2008 :  
<http://lists.gnu.org/archive/html/gnutls-devel/2008-05/msg00060.html>
- Note de version FileZilla 3.010 du 20 mai 2008 :  
[http://sourceforge.net/project/shownotes.php?release\\_id=600646](http://sourceforge.net/project/shownotes.php?release_id=600646)
- Site de téléchargement du projet FileZilla :  
[http://sourceforge.net/project/showfiles.php.group\\_id=21558](http://sourceforge.net/project/showfiles.php.group_id=21558)
- Bulletin de sécurité Gentoo GLSA-200805-20 du 21 mai 2008 :  
<http://www.gentoo.org/security/en/glsa/glsa-200805-20.xml>
- Bulletin de sécurité Debian DSA-1581 du 20 mai 2008 :  
<http://www.debian.org/security/2008/dsa-1581>
- Bulletin de sécurité RedHat RHSA-2008:0489 du 20 mai 2008 :  
<http://rhn.redhat.com/errata/RHSA-2008-0489.html>
- Bulletin de sécurité RedHat RHSA-2008:0492 du 20 mai 2008 :  
<http://rhn.redhat.com/errata/RHSA-2008-0492.html>
- Bulletin de sécurité Ubuntu USN-613-1 du 21 mai 2008 :  
<http://www.ubuntu.com/usn/usn-613-1>
- Référence CVE CVE-2008-1948 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1948>
- Référence CVE CVE-2008-1949 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1949>
- Référence CVE CVE-2008-1950 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1950>

## Gestion détaillée du document

**22 mai 2008** version initiale.

**18 septembre 2008** ajout des références aux bulletins de sécurité Gentoo, RedHat, Debian et Ubuntu.