



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 26 novembre 2009  
N° CERTA-2009-AVI-518

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans la bibliothèque libtool

---

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-2009-AVI-518>

---

### Gestion du document

Référence	CERTA-2009-AVI-518
Titre	Vulnérabilité dans la bibliothèque libtool
Date de la première version	26 novembre 2009
Date de la dernière version	–
Source(s)	Annonce de mise à jour Libtool du 16 novembre 2009
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

Élévation de privilèges.

## 2 Systèmes affectés

GNU Libtool 1.5.x.

## 3 Résumé

Une vulnérabilité dans la bibliothèque libtool peut être exploitée par un utilisateur local afin d'élever ses privilèges sur le système.

## 4 Description

La vulnérabilité est causée par un manque de contrôle des arguments fournis par l'utilisateur. Elle peut être exploitée par une personne malveillante, ayant un accès local au système, afin d'élever ses privilèges.

## 5 Solution

La mise à jour de sécurité est d'ores et déjà incluse dans la version courante de GNU Libtool au moyen du gestionnaire de version `git`.

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

## 6 Documentation

- Annonce de mise à jour de sécurité de GNU Libtool du 16 novembre 2009 :  
<http://lists.gnu.org/archive/html/libtool/2009-11/msg00066.html>
- Mise à jour de sécurité présente dans le gestionnaire de version `git` :  
<http://git.savannah.gnu.org/cgi/libtool.git/commit/?h=branch-1-5&id=29b48580df75f0c5vaa2962548a4c101ec7ed7ec>
- Référence CVE CVE-2009-3736 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3736>

## Gestion détaillée du document

**26 novembre 2009** version initiale.