Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 septembre 2009
N° CERTA-2009-AVI-361

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

## Objet : Vulnérabilité dans Dnsmasq



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2009-AVI-361 |
| Titre | Vulnérabilité dans Dnsmasq |
| Date de la première version | 01 septembre 2009 |
| Date de la dernière version | – |
| Source(s) | Liste des changements apportés à la version 2.50 de Dnsmasq |
| 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

Dnsmasq versions 2.49 et antérieures.

## 3 Résumé

Plusieurs vulnérabilités présentes dans `Dnsmasq` permettent à un utilisteur distant de provoquer un déni de service ou d'exécuter du code arbitraire.

## 4 Description

Deux vulnérabilités sont présentes dans `Dnsmasq`. Elles sont relatives à la mise en œuvre du protocole `TFTP` et permettent à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire. `Dnsmasq` doit être compilé avec le support du protocole `TFTP` pour que la faille soit exploitable.

# 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).
La version 2.50 corrige le problème :
http://www.thekelleys.org.uk/dnsmasq/

# 6 Documentation

- Liste des changements apportés à la version 2.50 de Dnsmasq :
  http://www.thekelleys.org.uk/dnsmasq/CHANGELOG
- Référence CVE CVE-2009-2957 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2957
- Référence CVE CVE-2009-2958 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2958

# Gestion détaillée du document

**01 septembre 2009** version initiale.