



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 25 juillet 2008  
N° CERTA-2008-AVI-375

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans dnsmasq

---

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-375>

---

### Gestion du document

Référence	CERTA-2008-AVI-375
Titre	Multiples vulnérabilités dans dnsmasq
Date de la première version	25 juillet 2008
Date de la dernière version	–
Source(s)	Annonces de mise à jour des versions 2.43, 2.44 et 2.45 de juillet 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

- Dénis de service à distance ;
- contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

Les versions antérieures à la 2.45.

## 3 Résumé

Deux vulnérabilités permettant une modification arbitraire du cache DNS et un déni de service à distance ont été corrigées dans dnsmasq.

## 4 Description

Une faiblesse dans l'aléa du choix des identifiants de transactions et des numéros de ports sources permet la modification arbitraire du cache DNS via des requêtes spécifiquement construites. De plus, une vulnérabilité lors du renouvellement du bail DHCP d'un client est exploitable pour provoquer un déni de service à distance.

## 5 Solution

Se référer au bulletin d'annonces de mise à jour de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Annonces de mise à jour des versions 2.43, 2.44 et 2.45 de juillet 2008 :  
<http://thekelleys.org.uk/dnsmask/CHANGELOG>
- Référence CVE CVE-2008-1447 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1447>

## Gestion détaillée du document

25 juillet 2008 version initiale.