

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans les mises en œuvres du protocole DNS

---

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-2006-AVI-173>

---

### Gestion du document

Référence	CERTA-2006-AVI-173
Titre	Multiples vulnérabilités dans les mises en œuvres du protocole DNS
Date de la première version	27 avril 2006
Date de la dernière version	–
Source(s)	Avis du NISCC
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

Déni de service à distance.

## 2 Systèmes affectés

Plusieurs logiciels de serveur de DNS.

## 3 Description

L'équipe *Oulu University Secure Programming Group* a créé une suite de tests du protocole DNS. Cette suite de test a permis de découvrir de nombreuses vulnérabilités dans les logiciels qui mettent en œuvre le protocole DNS. Les problèmes mis en évidence concernent les logiciels et non le protocole en lui-même.

L'identification des vulnérabilités dépend du degré de coopération entre les éditeurs de logiciels et l'équipe qui a réalisé les tests. Cependant quelques vulnérabilités ont déjà été découvertes et font l'objet de correctifs.

La liste à jour des logiciels testés et des correctifs disponibles se trouve sur le site du NISCC.

## **4 Solution**

Se référer au bulletin de sécurité des éditeurs identifiés dans l'avis du NISCC pour l'obtention des correctifs (cf. section Documentation).

## **5 Documentation**

- L'avis du NISCC :  
<http://www.niscc.gov.uk/niscc/docs/br-20060425-00311.html>

## **Gestion détaillée du document**

**27 avril 2006** version initiale.