



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 08 septembre 2006  
N° CERTA-2006-AVI-385-002

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités de BIND

---

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-385>

---

### Gestion du document

Référence	CERTA-2006-AVI-385-002
Titre	Vulnérabilités de BIND
Date de la première version	07 septembre 2006
Date de la dernière version	11 septembre 2006
Source(s)	Bulletin de mise à jour du Internet Systems Consortium (ISC)
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

Les versions de BIND antérieures à 9.3.2-P1, 9.2.6-P1 et 8.4.7 (ainsi que les versions Béta antérieures à 9.4.0b2, 9.3.3rc2, 9.2.7rc1 et 9.2.6-P1).

## 3 Description

ISC BIND (Berkeley Internet Name Domain) est un service pour la mise en œuvre du protocole DNS servant à la résolution de noms de domaine. Plusieurs vulnérabilités ont été identifiées dans ce dernier :

- il ne manipulerait pas de manière correcte certaines requêtes de type récursif (utilisées quand le serveur DNS se charge d'effectuer des requêtes itératives pour le client, aussi appelé *resolver*). Un utilisateur malveillant pourrait, à distance, profiter de cette vulnérabilité pour déclencher une erreur *INSIST*, en envoyant suffisamment de requêtes récursives : cette erreur arriverait tardivement, empêchant les autres clients d'obtenir une réponse du serveur à leurs requêtes.

- il ne manipulerait pas correctement des enregistrements (*Resource Record Sets*) liés aux extensions de sécurité DNS *DNSsec*. Un utilisateur malveillant pourrait construire des réponses DNS contenant plusieurs *SIG RRsets*, afin de perturber le fonctionnement du serveur auquel la réponse est adressée.

## 4 Solution

Se référer au bulletin de sécurité sur le site de l'ISC (*Internet Security Consortium*) pour l'obtention des correctifs (cf. section Documentation).

## 5 Documentation

- Site de téléchargement des différentes versions de Bind mises à jour :  
<http://www.isc.org/index.pl?sw/bind/>
- Bulletin de sécurité FreeBSD du 08 septembre 2006 :  
<http://security.freebsd.org/avisories/FreeBSD-SA-06:20.bind.asc>
- Bulletin de sécurité Ubuntu du 08 septembre 2006 :  
<http://www.ubuntu.com/usn/usn-343-1>
- Bulletin de sécurité Debian du 09 septembre 2006 :  
<http://www.debian.org/security/2006/dsa-1172>
- Bulletin de sécurité OpenBSD du 08 septembre 2006 :  
<http://www.openbsd.org/errata.html>
- Mise à jour Mandriva MDKSA-2006:163 du 08 septembre 2006 :  
<http://www.mandriva.com/security/advisories?name=MDKSA-2006:163>
- Référence CVE CVE-2006-4095 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4095>
- Référence CVE CVE-2006-4096 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4096>

## Gestion détaillée du document

**07 septembre 2006** version initiale ;

**08 septembre 2006** ajout des bulletins de sécurité FreeBSD et Ubuntu ;

**11 septembre 2006** ajout des bulletins de sécurité Debian, OpenBSD et Mandriva.