

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans BIND avec DNSSEC

---

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-2010-AVI-044>

---

### Gestion du document

Référence	CERTA-2010-AVI-044
Titre	Vulnérabilité dans BIND avec DNSSEC
Date de la première version	02 février 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité de l'ISC du 23 novembre 2009, mis à jour le 19 janvier 2010
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

Contournement de la politique de sécurité.

## 2 Systèmes affectés

- BIND versions 9.0.x ;
- BIND versions 9.1.x ;
- BIND versions 9.2.x ;
- BIND versions 9.3.x ;
- BIND versions 9.4.x antérieures à 9.4.3-P5 ;
- BIND versions 9.5.x antérieures à 9.5.2-P2 ;
- BIND versions 9.6.x antérieures à 9.6.1-P3 ;
- BIND version 9.7.0 beta.

## 3 Résumé

Une vulnérabilité dans le logiciel BIND avec DNSSEC permet la corruption du cache DNS.

## 4 Description

Le logiciel BIND avec DNSSEC activé ne sauvegarde pas correctement certains enregistrements dans son cache. Ce dysfonctionnement apparaît lorsque le client DNS effectue des requêtes DNSSEC (DO) sans vérification (CD). Cette vulnérabilité avait déjà été traitée dans l'avis CERTA-2009-AVI-515, mais le correctif s'est révélé insuffisant.

## 5 Solution

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

## 6 Documentation

- Document du CERTA CERTA-2009-AVI-515 du 26 novembre 2009 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-515/index.html>
- Bulletin de sécurité de l'ISC du 23 novembre 2009, mis à jour le 19 janvier :  
<https://www.isc.org/node/504>
- Référence CVE CVE-2009-4022 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4022>
- Référence CVE CVE-2010-0290 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0290>

## Gestion détaillée du document

02 février 2010 version initiale.