

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans ISC 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-2012-AVI-500>

---

### Gestion du document

Référence	CERTA-2012-AVI-500
Titre	Vulnérabilité dans ISC BIND
Date de la première version	13 septembre 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité ISC du 12 septembre 2012
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

ISC BIND versions :

- 9.0.x à 9.6.x ;
- 9.4-ESV à 9.4-ESV-R5-P1 ;
- 9.6-ESV à 9.6-ESV-R7-P2 ;
- 9.7.0 à 9.7.6-P2 ;
- 9.8.0 à 9.8.3-P2 ;
- 9.9.0 à 9.9.1-P2.

Les branches 9.4 et 9.5 sont également affectées mais ne sont plus maintenues.

## 3 Résumé

Une vulnérabilité a été corrigée dans *ISC BIND*. Elle concerne un déni de service à distance qui se déclenche lorsqu'un enregistrement avec un champ RDATA très grand est chargé par un serveur DNS.

## **4 Solution**

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

## **5 Documentation**

- Bulletin de sécurité ISC du 12 septembre 2012 :  
<https://kb.isc.org/article/AA-00778/74>
- Référence CVE CVE-2012-4244 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4244>

## **Gestion détaillée du document**

**13 septembre 2012** version initiale.