

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-2010-AVI-320>

Gestion du document

Référence	CERTA-2010-AVI-320
Titre	Vulnérabilité dans ISC Bind
Date de la première version	19 juillet 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité ISC du 15 juillet 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

Déni de service à distance.

2 Systèmes affectés

ISC Bind versions 9.7.1 et 9.7.1-P1.

3 Résumé

Une vulnérabilité dans le serveur *DNS* Bind permet à un utilisateur distant de provoquer un déni de service.

4 Description

Une erreur dans la mise en œuvre de *DNSSEC* est présente dans Bind. Ainsi, sous certaines conditions, un utilisateur distant malintentionné peut provoquer un déni de service par le biais d'une requête particulière d'un enregistrement de type *RRSIG* sur le serveur vulnérable.

5 Solution

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

6 Documentation

- Bulletin de sécurité ISC du 15 juillet 2010 :
<http://www.isc.org/software/bind/advisories/cve-2010-0213>
- Référence CVE CVE-2010-0213 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0213>

Gestion détaillée du document

19 juillet 2010 version initiale.