Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 mai 2011
N° CERTA-2011-AVI-279

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-2011-AVI-279

Gestion du document

Référence	CERTA-2011-AVI-279
Titre	Vulnérabilité dans ISC BIND
Date de la première version	06 mai 2011
Date de la dernière version	–
Source	Bulletin de sécurité ISC du 05 mai 2011
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, version 9.8.0.

3 Résumé

Une vulnérabilité dans ISC BIND est exploitable par une utilisateur malveillant pour provoquer un déni de service à distance.

4 Description

Quand la fonctionnalité de substitution de réponse DNS, RPZ, est utilisée, une requête spécialement conçue peut déclencher la terminaison du serveur de noms de domaine.

Ce problème est également provoqué par des serveurs non malveillants utilisant DNSSEC.

5 Solution

La version 9.8.0-P1 d'ISC BIND corrige ce problème.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité ISC du 05 mai 2011 :
  https://www.isc.org/CVE-2011-1907
- Référence CVE CVE-2011-1907 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1907

Gestion détaillée du document

06 mai 2011 version initiale.