Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 mai 2007
N° CERTA-2007-AVI-199

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de BIND

Gestion du document

Référence	CERTA-2007-AVI-199
Titre	Vulnérabilité de BIND
Date de la première version	02 mai 2007
Date de la dernière version	–
Source(s)	Avis ISC du 30 avril 2007
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

BIND, versions 9.4.x et 9.5.x.

3 Résumé

Une vulnérabilité de *BIND* permet à un utilisateur malveillant de provoquer un déni de service à distance.

4 Description

BIND est un logiciel DNS couramment utilisé.

Une erreur dans l'appel de la fonction `query_addsoa()` peut provoquer un arrêt du programme. Ce comportement peut être exploité pour provoquer un déni de service à distance.

L'exploitation de la vulnérabilité n'est pas possible si la recherche récursive est desactivée. Cette désactivation se traduit par le paramétrage `recursion no` dans le fichier de configuration `named.conf`.

5 Solution

Mettre à jour le logiciel dans la version 9.4.1 ou 9.5.0a4. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de l'ISC du 30 avril 2007 :
  http://www.isc.org/sw/bind/bind-security.php
- Site de téléchargement de la version 9.4.1 de BIND :
  ftp://ftp.isc.org/isc/bind9/9.4.1/bind-9.4.1.tar.gz
  ftp://ftp.isc.org/isc/bind9/9.4.1/bind-9.4.1.zip
  ftp://ftp.isc.org/isc/bind9/9.4.1/bind-9.4.1.debug.zip
- Référence CVE CVE-2007-2241 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2241

Gestion détaillée du document

02 mai 2007 version initiale.