Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 juin 2002
N° CERTA-2002-AVI-116

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Déni de service sur BIND 9

Gestion du document

Référence	CERTA-2002-AVI-116
Titre	Déni de service sur BIND 9
Date de la première version	05 juin 2002
Date de la dernière version	–
Source(s)	Avis CA-2002-15 du CERT/CC
Pièce(s) jointe(s)	Aucune

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Déni du service DNS assuré par BIND avec incidences sur tous les protocoles l'utilisant (HTTP, SMTP,...).

2 Systèmes affectés

Tout système utilisant BIND 9 dans une version antérieure à la 9.2.1 (versions 4 et 8 non affectées).

3 Résumé

Il est possible de fabriquer un paquet DNS qui, envoyé au serveur, provoquera son arrêt.

4 Description

Lorsque certains tests de cohérence échouent sur un message, le serveur s'arrête au lieu de simplement rejeter la requête. Des paquets peuvent donc être créés pour déclencher ce comportement et obtenir un déni de service.

5 Solution

Mettre à jour BIND 9 avec une version au moins égale à la 9.2.1.

- Sources
  http://www.isc.org/products/BIND/bind9.html
- Red Hat Linux
  http://rhn.redhat.com/errata/RHSA-2002-105.html
- Mandrake Linux
  http://www.linux-mandrake.com/en/security/2002/MDKSA-2002-038.php

6 Documentation

Avis du CERT/CC
http://www.kb.cert.org/vuls/id/739123

Gestion détaillée du document

05 juin 2002 version initiale.