Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 septembre 2010
N° CERTA-2010-AVI-459

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans BIND

Gestion du document

Référence	CERTA-2010-AVI-459
Titre	Multiples vulnérabilités dans BIND
Date de la première version	30 septembre 2010
Date de la dernière version	–
Source(s)	Note de mise à jour de BIND 9.7.2-P2
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

ISC BIND versions 9.7.x

3 Résumé

Deux vulnérabilités dans `ISC BIND 9.7.x` permettent, entre autres, un déni de service à distance, ainsi que l'accès à des données de cache du DNS.

4 Description

Deux vulnérabilités ont été identifiées dans `ISC BIND 9.7.x`:

- une erreur peut permettre un accès au cache du DNS, et cela même si ces données sont protégées par des régles de contrôle d'accès. Il est nécessaire que le serveur DNS fonctionne à la fois en mode récursif et fasse authorité *authoritative* pour que cette vulnérabilité soit exploitable ;

– lors de la validation d'une requête DNSSEC, un déni de service à distance est possible sous certaines conditions.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).
La version 9.7.2-P2, disponible sur le site de l'éditeur, corrige ces vulnérabilités.

6 Documentation

– Avis de sécurité concernant BIND 9.7.2 :
https://lists.isc.org/pipermail/bind-announce/2010-September/000655.html
– Note de mise à jour de la version ISC BIND 9.7.2-P2 :
http://ftp.isc.org/isc/bind9/9.7.2-P2/RELEASE-NOTES-BIND-9.7.2-P2.html

Gestion détaillée du document

30 septembre 2010 version initiale.