

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans BIND avec DNSSEC

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-2009-AVI-515>

Gestion du document

Référence	CERTA-2009-AVI-515-002
Titre	Vulnérabilité dans BIND avec DNSSEC
Date de la première version	26 novembre 2009
Date de la dernière version	12 janvier 2010
Source(s)	Bulletin de sécurité de l'ISC du 23 novembre 2009
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

Contournement de la politique de sécurité.

2 Systèmes affectés

- BIND versions 9.0.x ;
- BIND versions 9.1.x ;
- BIND versions 9.2.x ;
- BIND versions 9.3.x ;
- BIND versions 9.4.x antérieures à 9.4.3-P4 ;
- BIND versions 9.5.x antérieures à 9.5.2-P1 ;
- BIND versions 9.6.x antérieures à 9.6.1-P2.

3 Résumé

Une vulnérabilité dans le logiciel BIND avec DNSSEC permet la corruption du cache DNS.

4 Description

Le logiciel BIND avec DNSSEC activé ne sauvegarde pas correctement certains enregistrements dans son cache. Ce dysfonctionnement apparaît lorsque le client DNS effectue des requêtes DNSSEC (DO) sans vérification (CD).

5 Solution

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

6 Documentation

- Référence CVE CVE-2009-4022 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4022>
- Bulletin de sécurité de l'ISC du 23 novembre 2009 :
<https://www.isc.org/node/504>
- Bulletin de sécurité Sun du 24 novembre 2009 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-273169-1>
- Bulletin de sécurité FreeBSD du 06 janvier 2010 :
<http://security.freebsd.org/advisories/FreeBSD-SA-10:01.bind.asc>

Gestion détaillée du document

26 novembre 2009 version initiale ;

27 novembre 2009 ajout du bulletin de sécurité Sun ;

12 janvier 2010 ajout du bulletin de sécurité FreeBSD.