

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-320>

Gestion du document

Référence	CERTA-2011-AVI-320
Titre	Vulnérabilité dans Bind
Date de la première version	27 mai 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Bind CVE-2011-1910 du 26 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

- Bind versions 9.4-ESV-R3 et suivantes ;
- Bind versions 9.6-ESV-R2 et suivantes ;
- Bind versions 9.6.3 et suivantes ;
- Bind versions 9.7.1 et suivantes ;
- Bind versions 9.8.0 et suivantes.

3 Résumé

Une vulnérabilité dans Bind permet à un utilisateur distant malintentionné de provoquer un déni de service.

4 Description

Une vulnérabilité est présente dans le serveur DNS Bind. Elle est relative à la mise en œuvre d'un système de cache négatif des enregistrements invalides dans un contexte de DNSSEC. Cette faille permet à un utilisateur distant malintentionné de provoquer un déni de service au moyen d'un serveur DNSSEC autorisé construit de façon particulière.

5 Solution

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

6 Documentation

- Bulletin de sécurité Bind CVE-2011-1910 du 26 mai 2011 :
<http://www.isc.org/software/bind/advisories/cve-2011-1910>
- Référence CVE CVE-2011-1910 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1910>

Gestion détaillée du document

27 mai 2011 version initiale.