

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans ISC 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-2008-AVI-039>

Gestion du document

Référence	CERTA-2008-AVI-039
Titre	Vulnérabilité dans ISC BIND
Date de la première version	28 janvier 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité ISC du 18 janvier 2008
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

- Exécution de code arbitraire ;
- déni de service.

2 Systèmes affectés

- BIND 8.x (toutes versions) ;
- BIND 9.0 (toutes versions) ;
- BIND 9.1 (toutes versions) ;
- BIND 9.2 (toutes versions) ;
- BIND 9.3.0, 9.3.1, 9.3.2, 9.3.3, 9.3.4 ;
- BIND 9.4.0, 9.4.1, 9.4.2 ;
- BIND 9.5.0a1, 9.5.0a2, 9.5.0a3, 9.5.0a4, 9.5.0a5, 9.5.0a6, 9.5.0a7, 9.5.0b1.

3 Résumé

Une vulnérabilité dans ISC BIND permet à un utilisateur malintentionné de provoquer un déni de service ou potentiellement d'exécuter du code arbitraire.

4 Description

Une faille a été identifiée dans une fonction de la bibliothèque `libbind` fournie avec le serveur DNS : BIND. Cette vulnérabilité peut conduire à une corruption de mémoire permettant ainsi à un utilisateur malintentionné de provoquer un déni de service ou, selon l'éditeur, d'exécuter du code arbitraire.

Il est à noter que la fonction vulnérable n'étant pas mise en œuvre par BIND lui-même, le serveur n'est pas vulnérable. Seules des applications s'appuyant sur la bibliothèque `libbind` et sur cette fonction seront vulnérables.

5 Solution

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

6 Documentation

- Bulletin de sécurité ISC BIND du 18 janvier 2008 :
<http://www.isc.org/index.pl?sw/bind/bind-security.php>
- Référence CVE CVE-2008-0122 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0122>

Gestion détaillée du document

28 janvier 2008 version initiale.