



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 mars 2007
N° CERTA-2007-AVI-056-006

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du serveur DNS 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-2007-AVI-056>

Gestion du document

Référence	CERTA-2007-AVI-056-006
Titre	Vulnérabilité du serveur DNS BIND
Date de la première version	26 janvier 2007
Date de la dernière version	28 mars 2007
Source(s)	Annonce de l'Internet Systems Consortium (ISC) Security du 25 janvier 2007
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

- ISC BIND 9.0.x, toutes les versions ;
- ISC BIND 9.1.x, toutes les versions ;
- ISC BIND 9.2.x, pour les versions de 9.2.0 à 9.2.7 comprise ;
- ISC BIND 9.3.x, pour les versions de 9.3.0 à 9.3.3 comprise ;
- ISC BIND 9.4.0, pour les versions de 9.4.0a1 à 9.4.0a6 comprise ;
- ISC BIND 9.4.0, pour les versions de 9.4.0b1 à 9.4.0b4 comprise, et 9.4.0rc1 ;
- ISC BIND 9.5.0a1.

3 Résumé

Une vulnérabilité a été identifiée dans le serveur de résolution de noms de domaines DNS BIND. Une personne malveillante pourrait exploiter celle-ci, afin de provoquer un dysfonctionnement du service.

4 Description

Une vulnérabilité a été identifiée dans BIND. ISC BIND (pour *Berkeley Internet Name Domain*) est un service pour la mise en œuvre du protocole DNS servant à la résolution de noms de domaine.

L'application ne manipulerait pas correctement certaines requêtes de validation DNSSEC. Il s'agit d'un protocole (défini par le RFC 4033), considérant certains aspects de sécurité pour l'échange de données nécessaire à DNS.

Une personne malveillante pourrait donc exploiter cette vulnérabilité, afin de provoquer un dysfonctionnement du service fourni par BIND.

5 Solution

Se référer aux mises à jour de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Debian DSA 1254 du 27 janvier 2007 :
<http://www.debian.org/security/2007/dsa-1254>
- Bulletin de sécurité Fedora FEDORA-2007-147 du 29 janvier 2007 :
<http://fedoraneews.org/cms/node/2507>
- Bulletin de sécurité Mandriva MDKSA-2007:030 du 30 janvier 2007 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:030>
- Bulletin de sécurité SuSE SUSE-SA:2007:014 du 30 janvier 2007 :
<http://lists.suse.com/archive/suse-security-announce/2007-Jan/0016.html>
- Bulletin de sécurité Fedora FEDORA-2007-164 du 31 janvier 2007 :
<http://fedoraneews.org/cms/node/2537>
- Bulletin de sécurité Gentoo GLSA-200702-06/bind du 17 février 2007 :
<http://www.gentoo.org/security/en/glsa/glsa-200702-06.xml>
- Bulletin de sécurité Avaya ASA-2007-125 du 27 mars 2007 :
<http://support.avaya.com/elmodocs2/security/ASA-2007-125.htm>
- Référence CVE CVE-2007-0493 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0493>
- Référence CVE CVE-2007-0494 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0494>
- Page du projet ISC BIND :
<http://www.isc.org/products/BIND/>
- Annonces de sécurité ISC BIND :
<http://www.isc.org/index.pl?sw/bind/bind-security.php>
- Annonce de la vulnérabilité par ISC BIND :
<http://marc.theaimsgroup.com/?l=bind-announce&m=116968519300764&w=2>

Gestion détaillée du document

26 janvier 2007 version initiale.

29 janvier 2007 ajout de la référence CVE 2007-0493 et du bulletin de sécurité Debian.

30 janvier 2007 ajout de la référence du bulletin de sécurité Fedora.

31 janvier 2007 ajout des références aux bulletins de sécurité Mandriva et SuSE.

01 février 2007 ajout de la référence au bulletin de sécurité Fedora.

19 février 2007 ajout de la référence au bulletin de sécurité Gentoo.

28 mars 2007 ajout de la référence au bulletin de sécurité Avaya.