

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des serveurs 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-2005-AVI-033>

Gestion du document

Référence	CERTA-2005-AVI-033-002
Titre	Vulnérabilité des serveurs DNS BIND
Date de la première version	27 janvier 2005
Date de la dernière version	10 juin 2005
Source(s)	Avis 20050125-00059 et 20050125-00060 du NISCC
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.

2 Systèmes affectés

Tout système offrant un service DNS par l'intermédiaire de *BIND* en versions 8.4.4, 8.4.5 et 9.3.0.

3 Résumé

Un utilisateur distant mal intentionné peut provoquer l'arrêt du service DNS (et par ricochet de tout service utilisant la résolution de nom), en abusant d'une faille concernant soit les versions 8.4.4 et 8.4.5, soit la version 9.3.0.

4 Description

- Versions 8.4.4 et 8.4.5 (CAN-2005-0033) :
les interrogations déjà réalisées sont stockées dans un tableau dont les limites mémoire sont mal gérées et peuvent donc provoquer un déni de service par débordement.

- Version 9.3.0 (CAN-2005-0034) :
Un test de validation DNSSEC est basé sur un postulat incorrect et peut donc interrompre le service lors d'une requête légitime d'après la norme.

5 Contournement provisoire

- Versions 8.4.4 et 8.4.5 :
Désactiver l'interrogation récursive («recursion»), s'il ne s'agit pas d'un serveur cache, ainsi que la récupération des enregistrements annexes («glue fetching» : récupération de l'adresse IP en sus lors d'une interrogation NS, par exemple).
- Version 9.3.0 :
Désactiver DNSSEC ou simplement la validation DNSSEC dans les options.

6 Solution

Mettre à jour les sources en version 8.4.6 ou 9.3.1beta2 au moins.

7 Documentation

- Site Internet d'ISC *BIND* :
<http://www.isc.org>
- Bulletin de sécurité 20050125-00059 du NISCC sur *BIND 8* :
<http://www.niscc.gov.uk/niscc/docs/al-20050125-00059.html>
- Note de vulnérabilité #327633 de l'US-CERT sur *BIND 8* :
<http://www.kb.cert.org/vuls/id/327633>
- Bulletin de sécurité 20050125-00060 du NISCC sur *BIND 9* :
<http://www.niscc.gov.uk/niscc/docs/al-20050125-00060.html>
- Note de vulnérabilité #938617 de l'US-CERT sur *BIND 9* :
<http://www.kb.cert.org/vuls/id/938617>
- Bulletin de sécurité Mandrake MDKSA-2005:023 du 26 janvier 2005 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:023>
- Mise à jour de sécurité des paquetages NetBSD bind8 et bind9 :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/net/bind8/README.html>
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/net/bind9/README.html>
- Bulletin de sécurité FreeBSD FreeBSD-SA-05:12 du 09 juin 2005 :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:12.bind9.asc>
- Référence CVE CAN-2005-1278 :
- Référence CVE CAN-2005-0034 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0034>

Gestion détaillée du document

27 janvier 2005 version initiale.

31 janvier 2005 ajout de la référence CVE et des références aux bulletins de sécurité Mandrake et NetBSD.

10 juin 2005 ajout de la référence au bulletin de sécurité FreeBSD.