

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités sur les serveurs DNS BIND 4 et 8

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-2002-AVI-246>

Gestion du document

Référence	CERTA-2002-AVI-246-001
Titre	Multiples vulnérabilités sur les serveurs DNS BIND 4 et 8
Date de la première version	13 novembre 2002
Date de la dernière version	19 novembre 2002
Source(s)	Avis Internet Security Systems du 12 novembre 2002
Pièce(s) jointe(s)	Aucune

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

Tout système offrant un service DNS à l'aide de BIND version 4 (4.9.5 à 4.9.10) ou 8 (8.1, 8.2 à 8.2.6 et 8.3.0 à 8.3.3).

3 Résumé

Trois failles différentes ont été identifiées dans la fonction cache de BIND. Elles nécessitent que la récursivité ("recursion" : capacité à conduire une résolution à la place des clients) soit activée, ce qui est le cas par défaut. L'une d'entre elles permet l'exécution de code arbitraire avec les privilèges du service, les deux autres l'arrêt du service.

4 Description

L'avis d'ISS identifie les problèmes suivants :

- Il existe un débordement de mémoire dans la gestion des enregistrements ("rr, resource record") de type

SIG (RFC 2535) au sein du cache. Un utilisateur mal intentionné contrôlant un DNS autorité pour une zone pourrait alors exécuter du code arbitraire.

- En fabriquant une réponse UDP de grande taille, pour un sous-domaine inexistant ou un domaine dont les DNS autorités sont inaccessibles, il est possible de mettre fin au service.
- Comme dans le premier cas, le contrôle d'un DNS autorité permet de fabriquer des enregistrements SIG avec une date d'expiration invalide, pour lesquels une mauvaise gestion du cache conduit à désallouer deux fois la mémoire correspondant et donc à l'arrêt du service.

5 Contournement provisoire

Pour les rares cas où cela est possible (caches DNS ne répondant que pour les domaines dont ils sont autorité), désactiver la récursivité :

- BIND 4 : dans *named.boot* inclure *options no-recursion*.
- BIND 8 : dans *named.conf* inclure *recursion no*; dans l'entrée *options {}*.

Dans le cas de BIND 8, il est possible de restreindre les adresses IP pour lesquelles la récursivité est autorisée : utiliser une entrée de la forme *allow-recursion { adresse/masque; }* où adresse/masque correspond aux adresses pour lesquelles l'usage du cache est légitime. Sans supprimer les vulnérabilités, cette option limite les opportunités de les activer.

6 Solution

- Migrer vers BIND 9 ou un autre programme de service DNS.
- Mise à jour par ISC des fichiers sources :
 - Bind 8 :
<http://www.isc.org/products/BIND/bind8.html>
 - Bind 4 :
<http://www.isc.org/products/BIND/bind4.html>
- Red Hat Linux 6.2, 7.0, 7.1, 7.2 et 7.3
<http://rhn.redhat.com/errata/RHSA-2002-133.html>
- Linux Mandrake 7.2
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2002:077>
- Debian Linux
<http://www.debian.org/secuirty/2002/dsa-196>
- SuSE Linux 7.0, 7.1, 7.2, 7.3, 8.0 et 8.1
http://www.suse.com/de/security/2002_004_bind8.html
- Conectiva Linux 6.0
<http://distro.conectiva.com/atualizacoes/?id=a&anuncio=000546>
- OpenBSD 3.0, 3.1 et 3.2 (attention les versions 2 ne sont plus maintenues)
<http://www.openbsd.com/errata.html#named>
- FreeBSD 4.4, 4.5, 4.6 et 4.7
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-02%3A43.bind.asc>

7 Documentation

- Avis de sécurité ISS :
<http://bvlive01.iss.net/issEn/delivey/xforce/alertdetail.jsp?uid=21469>
- Vulnérabilités BIND recensées par ISC et point de contact :
<http://www.isc.org/products/BIND/bind-security.html>
- Syntaxe de l'entrée options dans BIND 8 :
<http://www.isc.org/products/BIND/docs/config/options.html>

Gestion détaillée du document

13 novembre 2002 version initiale.

19 novembre 2002 rajout de correctifs constructeurs.