Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 novembre 2000
N° CERTA-2000-AVI-071

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de BIND

Gestion du document

Référence	CERTA-2000-AVI-071
Titre	Multiples vulnérabilités de BIND
Date de la première version	14 novembre 2000
Date de la dernière version	–
Source(s)	Avis de sécurité de l'Internet Software Consortium Avis CA-2000-20 du CERT/CC
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

- Plusieurs dénis de service,
- Accès à distance avec privilèges.

2 Systèmes affectés

Tous les Systèmes Unix et Linux utilisant BIND versions 8.2.2 et 8.2.2-P1 à P6.

3 Résumé

Plusieurs vulnérabilités de BIND permettent à un utilisateur mal intentionné de bloquer le serveur de Nom (DNS).

4 Description

BIND est un *démon* de service de nom (DNS) trés répandu.

De nouvelles vulnérabilités ont été découvertes sur BIND. Elles permettent de bloquer les serveurs DNS.

- Une utilisation détournée de *zxfer*, grâce aux outils de transfert de zone (named-xfer et dig) présents dans la distribution de BIND, permet de bloquer le serveur de nom d'un site à distance.
- Une mauvaise implémentation de l'outil de vérification des signatures entraîne une division par zéro qui bloque le serveur. Cette erreur n'est pas présente dans le la version 8.2.2-P6 (corrigée avec le service pack 6) de BIND.
- Une erreur dans la façon de gérer les pointeurs dans les tables lors de l'utilisation de la compression peut entraîner l'entrée du programme dans une boucle infinie qui bloque elle aussi le serveur.
- Beaucoup d'autres vulnérabilités sont présentes dans les versions antérieures à 8.2.2-P1 (service pack 1) incluant les versions 8.2.1 et inférieures. En particulier, un accès à distance avec les privilèges de l'administrateur du service BIND est possible à l'aide d'un script, et de multiples autres vulnérabilités provoquant des dénis de service sont exploités.

5 Contournement provisoire

Pour éviter d'être corrompu par une machine utilisant la vulnérabilité *zxfer*, n'autoriser l'exécution d'un transfert de zone que depuis les machines de confiance (serveurs du domaine parent, ou bien serveur(s) secondaire(s) autoritaire(s) de la zone).

6 Solution

Télécharger les sources du correctif à appliquer (*Service Pack* 7) :
ftp://ftp.isc.org/isc/bind/src/8.2.2-P7/bindsrc.tar.gz
Ou bien appliquer le correctif proposé par votre éditeur du système sur lequel BIND est installé (Voir les avis de sécurité par éditeur dans le paragraphe documentation).

7 Documentation

- L'avis de l'ISC :
  http://www.isc.org/products/BIND/bind-security.html
- l'avis du CERT/CC :
  http://www.cert.org/advisories/CA-2000-20.html
- l'avis de Debian :
  http://www.debian.org/security/2000/20001112
- l'avis de Caldera Systems :
  http://www.calderasystems.com/support/security/advisories/CSSA-2000-04.0.0.txt
- celui de Linux-Mandrake :
  http://www.linux-mandrake.com/en/updates/MDKSA-2000-067.php3?dis=7.2

Gestion détaillée du document

14 novembre 2000 version initiale.