Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 août 2002
N° CERTA-2002-AVI-139-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de souches client DNS

Gestion du document

Référence	CERTA-2002-AVI-139-004
Titre	Vulnérabilité de souches client DNS
Date de la première version	28 juin 2002
Date de la dernière version	19 août 2002
Source(s)	Avis FreeBSD-SA-02:28.resolv de FreeBSD
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 à distance.

2 Systèmes affectés

Tous les systèmes utilisant une souche client DNS issue de ISC BIND.

3 Résumé

Une vulnérabilité de type débordement de mémoire présente dans certaines souches client DNS permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance, par le biais d'un serveur DNS hostile, sur le poste du client vulnérable.

4 Description

Le DNS (Domain Name System) est un mécanisme utilisé pour la résolution de nom de machines (exemple : www.certa.ssi.gouv.fr) en adresse IP et vice-versa.

Un utilisateur mal intentionné peut configurer un serveur DNS hostile pour renvoyer des réponses aux requêtes DNS qui provoqueront un débordement de mémoire lors de l'interprétation réalisée par les souches client DNS vulnérables.

Ce débordement de mémoire permet, sous certaines conditions, de réaliser l'exécution de code arbitraire sur le poste du client avec les privilèges de l'utilisateur exécutant l'application qui fait appel à la souche client DNS vulnérable.

5 Solution

Consultez l'éditeur pour la mise à jour correspondant à votre système :

- FreeBSD :
  ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-02:28.resolv.asc
- OpenBSD :
  http://www.openbsd.org/errata.html#resolver
- NetBSD :
  ftp://ftp.NetBSD.ORG/pub/NetBSD/security/advisories/NetBSD-SA2002-006.txt.asc
- IRIX :
  http://www.sgi.com/support/security/advisories/2002/0701-01-I
- Mandrake :
  http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-043.php
- Suse :
  http://lists2.suse.com/archive/suse-security-announce/2002-Jul/0002.html
- SUN :
  http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F46042&zone_32=category%3Asecurity
- RedHat :
  http://rhn.redhat.com/errata/RHSA-2002-133.html
- Mandrake :
  http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-050.php
- HP (se référer au bulletin HPSBUX0208-209):
  http://itrc.hp.com

6 Documentation

- Avis de sécurité "Buffer overflow in resolver" de FreeBSD :
  ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-02:28.resolv.asc
- Avis de sécurité "Multiple vendor's DNS stub resolvers vulnerable to buffer overflow " du CERT/CC :
  http://www.kb.cert.org/vuls/id/803539
- Bulletin de sécurité #CA-2002-19 "Buffer Overflow in Multiple DNS Resolver Librairies" du CERT/CC :
  http://www.cert.org/advisories/CA-2002-19.html

Gestion détaillée du document

28 juin 2002 version initiale.

17 juillet 2002 ajout des avis CERT/CC, IRIX, Suse et Mandrake.

30 juillet 2002 ajout référence au bulletin Sun Alert Notification #46042 de SUN.

12 août 2002 ajout référence à l'avis RHSA-2002-133 de RedHat.

19 août 2002 ajout références aux avis de Mandrake et HP.