Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 novembre 2002
N° CERTA-2002-AVI-163-005

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les Sun RPC

Gestion du document

Référence	CERTA-2002-AVI-163-005
Titre	Vulnérabilité dans les Sun RPC
Date de la première version	01 août 2002
Date de la dernière version	21 novembre 2002
Source(s)	Bulletin de sécurité ISS
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

- Elévation de privilèges ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- Sun Microsystems Solaris 2.5.1 ;
- Sun Microsystems Solaris 2.6 ;
- Sun Microsystems Solaris 7 ;
- Sun Microsystems Solaris 8 ;
- Sun Microsystems Solaris 9 ;
- FreeBSD jusqu'à la version 4.6.1-RELEASE-p3 incluse ;
- OpenBSD version 2.0 à la version 3.1 incluse ;
- NetBSD version 1.4.* à la version 1.6 beta ;
- Toutes les versions de MIT Kerberos version 5 jusqu'à la version krb5-1.2.5 incluse ;
- Mac OS X ;
- OpenAFS version 1.0 à 1.2.5 et version 1.3.0 à 1.3.2.

3 Résumé

Une vulnérabilité a été découverte dans une primitive de filtrage XDR utilisée dans les Sun RPC.

4 Description

Sun RPC (Remote Procedure Call) est un protocole de type client/serveur utilisé pour l'implémentation d'applications réparties.

Celui-ci utilise de manière transparente le protocole XDR (eXternal Data Representation) afin de résoudre les problèmes de non unicité de représentation interne des objets entre différentes machines.

Une vulnérabilité de type débordement de mémoire à été découverte dans la primitive de filtrage `xdr_array` utilisée par de nombreux services RPC. Un utilisateur mal intentionné peut exploiter cette vulnérabilité afin d'exécuter du code arbitraire à distance avec les privilèges de l'utilisateur `root`.

Cette vulnérabilité est également présente dans de nombreuses applications utilisant des librairies dérivées de la librairie Sun RPC (libc, glibc ou dietlibc), notamment dans certains serveurs du système de fichiers distribué AFS (volserver, vlserver, ptserver, buserver) , ou bien le système d'administration de Kerberos 5 (kadmind).

5 Contournement provisoire

Le correctif pour `Sun solaris systems` est maintenant disponible. Il est toutefois conseillé de :

- filtrer l'accès au RPC Portmapper (111/TCP et UDP) ;
- filtrer l'accès à la plage des ports hauts utilisés par les services RPC ;
- d'arrêter les services RPC non utilisés.

6 Solution

Appliquer le correctif selon l'éditeur (cf. Documentation).

7 Documentation

Bulletin du CERT/CC :
http://www.cert.org/advisories/CA-2002-25.html

- Vulnérabilité dans la fonction xrd_array :
  - Bulletin de sécurité ISS :
    http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=20823
  - Bulletin de sécurité FreeBSD :
    ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-02:34.rpc.asc
  - Alerte OpenBSD :
    http://www.openbsd.org/security.html
  - Bulletin NetBSD :
    http://www.netbsd.org/security
  - Bulletin de sécurité SGI :
    ftp://patches.sgi.com/support/free/security/advisories/20020801-01-A
  - Bulletin de sécurité SUN :
    http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/46122&zone_32=category:security
  - Bulletin de sécurité Apple :
    http://www.info.apple.com/usen/security/security_updates.html
  - Bulletin de sécurité DEBIAN #146:
    http://www.debian.org/security/2002/dsa-146
  - Bulletin de sécurité DEBIAN #149:
    http://www.debian.org/security/2002/dsa-149

  - Bulletin de sécurité Red Hat :
    http://www.redhat.com/support/errata/RHSA-2002-166.html
  - Bulletin de sécurité SuSE-SA:2002:031 de SuSE :
    http://www.suse.com/de/security/2002_031_glibc.html

- Vunérabilité dans Kerberos :

  - Bulletin MIT Kerberos :
    http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2002-001-xdr.txt
  - Bulletin de sécurité DEBIAN #143:
    http://www.debian.org/security/2002/dsa-143

- Vulnérabilité dans AFS :

  - Bulletin de sécurité OpenAFS :
    http://www.openafs.org/security
  - Bulletin de sécurité DEBIAN #142:
    http://www.debian.org/security/2002/dsa-142

Gestion détaillée du document

01 août 2002 version initiale.
05 août 2002 ajout des bulletins de sécurité SUN, NetBSD, SGI, MIT Kerberos et Apple.
06 août 2002 ajout des bulletins du CERT/CC, OpenAFS et Debian.
19 août 2002 ajout des bulletins Debian, Red Hat et SGI.
03 septembre 2002 ajout du bulletin de SuSE.
17 octobre 2002 correction d'un lien.
21 novembre 2002 correction d'un lien.