Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 mai 2003
N° CERTA-2003-AVI-052-005

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les Sun RPC

Gestion du document

Référence	CERTA-2003-AVI-052-005
Titre	Vulnérabilité dans les Sun RPC
Date de la première version	20 mars 2003
Date de la dernière version	30 mai 2003
Source(s)	Avis CA-2003-10 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

- Exécution de code arbitraire à distance ;
- déni de service.

2 Systèmes affectés

Les Sun RPC ainsi que des bibliothèques dérivées du code d'origine sont disponibles sur de nombreuses plate-formes de type Unix ou Linux.

3 Résumé

Une vulnérabilité a été découverte dans la fonction `xdrmem_getbytes` 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 a été découverte dans la fonction `xdrmem_getbytes`. Un utilisateur mal intentionné peut exploiter cette vulnérabilité à travers une application utilisant cette fonction (telle `rpcbind` sous Solaris) afin d'exécuter du code arbitraire à distance ou réaliser un déni de service.

Cette vulnérabilité est également présente dans de nombreuses applications utilisant des bibliothèques dérivées de la bibliothèque Sun RPC (libc, glibc, etc.), notamment `kadmind`, le système d'administration de Kerberos 5.

5 Contournement provisoire

En attendant d'appliquer les correctifs, il est conseillé de :

- filtrer l'accès au RPC Portmapper (111/tcp et udp) ;
- filtrer l'accès aux applications RPC (correspondant généralement à la plage des ports hauts) ;
- arrêter les services RPC utilisant la fonction vulnérable ;
- arrêter les services RPC non utilisés.

6 Solution

Appliquer le correctif selon l'éditeur:

- Bulletin de sécurité 2003-03 du MIT :
  http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2003-003-xdr.txt
- Bulletin de sécurité HPSBUX0303-252 "Potential security vulnerability in xdrmem_getbytes()" de Hewlett-Packard :
  http://itrc.hp.com/cki/bin/doc.pl/screen=ckiSecurityBulletin
- Bulletin de sécurité MSS-OAR-E01-2003.0371 "Integer overflow in various RPC implementations" d'IBM :
  http://www-1.ibm.com/services/continuity/recover1.nsf/MSS/MSS-OAR-E01-2003.0371.1
- Bulletin de sécurité RHSA-2003:089 de Red Hat :
  https://rhn.redhat.com/errata/RHSA-2003-089.html
- Bulletin de sécurité RHSA-2003:051 de Red Hat :
  https://rhn.redhat.com/errata/RHSA-2003-051.html
- Bulletin de sécurité RHSA-2003:091 de Red Hat :
  https://rhn.redhat.com/errata/RHSA-2003-091.html
- Bulletin de sécurité #51884 de Sun :
  http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/51884
- Bulletin de sécurité FreeBSD-SA-03:05 "Remote denial-of-service in XDR encoder/decoder" de FreeBSD :
  ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-03%3A05.xdr.asc
- Bulletin de sécurité DSA-266 de Debian :
  http://www.debian.org/security/2003/dsa-266
- Bulletin de sécurité DSA-272 de Debian :
  http://www.debian.org/security/2003/dsa-272
- Bulletin de sécurité DSA-282 de Debian :
  http://www.debian.org/security/2003/dsa-282
- Bulletin de sécurité MDKSA-2003:037 de Mandrake :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:037
- Bulletin de sécurité MDKSA-2003:043 de Mandrake :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:043
- Bulletin de sécurité NetBSD-SA2003-008 de NetBSD :
  ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-008.txt.asc
- Bulletin de sécurité 200303-22 de gentoo :
  http://www.securityfocus.com/advisories/5161
- Bulletin de sécurité 200303-28 de gentoo :
  http://www.securityfocus.com/advisories/5203

- Bulletin de sécurité 200303-29 de gentoo :
  http://www.securityfocus.com/advisories/5206
- Bulletin de sécurité 20030402-01-P de SGI :
  ftp://patches.sgi.com/support/free/security/advisories/20030402-01-P
- Bulletin de sécurité SuSE-SA:2003:027 de SuSE :
  http://www.suse.com/de/security/2003_027_glibc.html

7 Documentation

- Avis CA-2003-10 "Integer overflow in Sun RPC library routines" du CERT/CC :
  http://www.cert.org/advisories/CA-2003-10.html
- Bulletin de sécurité "XDR Integer Overflow" de eEye Digital Security :
  http://www.eye.com/html/Research/Advisories/AD20030318.html
- Référence CVE CAN-2003-0028 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0028

Gestion détaillée du document

20 mars 2003 version initiale.

21 mars 2003 ajout références aux bulletins de Sun et FreeBSD. Mention pour rpcbind (Solaris).

27 mars 2003 ajout références aux bulletins de Debian, Mandrake, gentoo, NetBSD. Ajout référence CVE.

4 avril 2003 ajout références aux bulletins de Gentoo, Red Hat, Mandrake relatifs à kadmind. Ajout références aux bulletins de Gentoo, Debian relatifs à dietlibc.

10 avril 2003 ajout références aux bulletins de Debian et SGI relatifs à Glibc.

30 mai 2003 ajout référence au bulletin de SuSE relatif à Glibc.