CERT Advisory CA-1992-12 Revised Patch for SunOS /usr /etc/rpc.mountd Vulnerability


```
============================================================================
CA-92:12                      CERT Advisory
                              May 28, 1992
         Revised Patch for SunOS /usr/etc/rpc.mountd Vulnerability

- ----------------------------------------------------------------------------

                THIS ADVISORY AND CA-91:09 HAVE BEEN
                SUPERSEDED BY CERT ADVISORY CA-94:02

The Computer Emergency Response Team/Coordination Center (CERT/CC) has
received information concerning the availability of a revised security
patch for /usr/etc/rpc.mountd in Sun Microsystems Computer Corporation
operating systems.  This patch fixes an additional vulnerability that
was not addressed in CERT advisory CA-91:09.SunOS.rpc.mountd.vulnerability.

Sun has provided patches for SunOS 4.1, SunOS 4.1_PSR_A, SunOS 4.1.1,
and SunOS 4.1.2.  These patches are available through your local Sun
Answer Center as well as through anonymous ftp from ftp.uu.net (137.39.1.9)
in the /systems/sun/sun-dist directory.

Patch ID and file information are as follows:

Fix                     Patch ID       Filename            Checksum
/usr/etc/rpc.mountd     100296-02      100296-02.tar.Z     30606    23

Please note that Sun Microsystems sometimes updates patch files.  If you
find that the checksum is different, please contact Sun Microsystems or
the CERT/CC for verification.

- ----------------------------------------------------------------------------
I.   Description

     Under certain conditions an exported NFS filesystem can be
     mounted by any system on the Internet even though it may appear
     that access to the filesystem is restricted to specific hosts.

II.  Impact

     Unauthorized remote hosts will be able to mount the exported filesystem.

III. Solution

     As root:

     1.  Move the existing rpc.mountd aside and change the permissions.

         # mv /usr/etc/rpc.mountd /usr/etc/rpc.mountd.OLD
         # chmod 400 /usr/etc/rpc.mountd.OLD

     2.  Install the new version

         # cp `arch`/rpc.mountd /usr/etc
         # chown root.staff /usr/etc/rpc.mountd
         # chmod 755 /usr/etc/rpc.mountd

     3.  Kill the currently running rpc.mountd and restart it, or
         reboot the system.  In either case, systems with filesystems
         mounted from this host will have interruptions in service.

- ----------------------------------------------------------------------------

If you believe that your system has been compromised, contact CERT/CC or
your representative in FIRST (Forum of Incident Response and Security Teams).

Internet E-mail: cert@cert.org
Telephone: 412-268-7090 (24-hour hotline)
           CERT/CC personnel answer 7:30 a.m.-6:00 p.m. EST(GMT-5)/EDT(GMT-4),
           on call for emergencies during other hours.

Computer Emergency Response Team/Coordination Center (CERT/CC)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
```

Past advisories, information about FIRST representatives, and other
information related to computer security are available for anonymous ftp
from cert.org (192.88.209.5).

-----BEGIN PGP SIGNATURE-----
Version: PGP for Personal Privacy 5.0
Charset: noconv

iQA/AwUBOBS9v1r9kb5qlZHQEQJCzQCg9FJNR+GlY5SUM91foN8bKANqGLgAnRou
v/c5Xe73yT2H0U4H4DqdpmEo
=DXZB
-----END PGP SIGNATURE-----