# CERT Advisory CA-1994-04 SunOS /usr/ucb/rdist Vulnerability



==========
CERT Advisory CA-94:04
Original issue date:  March 17,  1994
Last revised: July 24, 1996
              SUPERSEDED BY CA-96:14

Topic:   SunOS /usr/ucb/rdist Vulnerability
==========
                *** SUPERSEDED BY CA-96:14 ***

The CERT Coordination Center has received information concerning a vulnerability in /usr/ucb/rdist in Sun Microsystems, Inc. SunOS 4.1.1, 4.1.2, 4.1.3, and 4.1.3c on all sun3 and sun4 architectures.  SunOS 4.1.3_U1, Solaris 2.x, and Solbourne's 4.1B and 4.1C are not vulnerable.

This is a Sun specific Advisory.  Please reference CERT Advisory CA-91:20 "/usr/ucb/rdist Vulnerability" for general information regarding other vendors.  A vendor status file pub/cert_advisories/rdist-patch-status is available via anonymous FTP from info.cert.org.

This vulnerability is being actively exploited; please review CERT Advisory CA-94:01 "Ongoing Network Monitoring Attacks."

Patches can be obtained from local Sun Answer Centers worldwide as well as through anonymous FTP from ftp.uu.net in the /systems/sun/sun-dist directory. In Europe, these patches are available from ftp.eu.net in the /sun/fixes directory.

Information concerning specific patches is outlined below. Please note that Sun sometimes updates patch files.  If you find that the checksum is different, please contact Sun.

- ----------

I.   Description

     A security vulnerability exists in /usr/ucb/rdist that can be used to gain unauthorized privileges.  Under some circumstances /usr/ucb/rdist can be used to create setuid root programs.

II.  Impact

     This vulnerability allows a local user to gain root access.

III. Solution

     A.  If rdist is not being used, change the permissions on the file.

         # chmod 700 /usr/ucb/rdist

     B.  Obtain and install the appropriate patches according to the instructions included with the patches.

         | Module | Patch ID | Filename |
         |---|---|---|
         | rdist | 100383-06 | 100383-06.tar.Z |

                BSD Checksum = 58984 121
                System V Checksum = 9125 241
                MD5 Checksum = f8f78ddab19af5efabb9bd66fc8f5c1a

- ----------

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

Internet E-mail: cert@cert.org
Telephone: 412-268-7090 (24-hour hotline)
           CERT personnel answer 8:30 a.m.-5:00 p.m. EST(GMT-5)/EDT(GMT-4),
           and are on call for emergencies during other hours.

CERT Coordination Center
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 info.cert.org.



~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Revision history

July 24, 1996  Superseded by CA-96.14

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

iQA/AwUBOBS98lr9kb5qlZHQEQI0jACeLDvLwg18iTYe+Q+wlBlsneWeUesAnRXy
oaD/1zhBGFnZeWBr1+tibSjp
=o1wZ
-----END PGP SIGNATURE-----
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~