CERT Advisory CA-1991-20 /usr/ucb/rdist Vulnerability

==========
CA-91:20 CERT Advisory
October 22, 1991
/usr/ucb/rdist Vulnerability

- ----------
*** SUPERSEDED BY CA-96.14 ***

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability in /usr/ucb/rdist (the location of rdist may vary depending on the operating system). This vulnerability is present in possibly all versions of rdist. Vendors responding with patches are listed below. Additionally, some vendors who do not include rdist in their operating systems are identified. Operating systems from vendors not listed in either of the two categories below will probably be affected and the CERT/CC has proposed a workaround for those systems.

VENDORS THAT DO NOT SHIP rdist
(Note: Even though these vendors do not ship rdist, it may have been added later (for example, by the system administrator). It is also possible that vendors porting one of these operating systems may have added rdist. In both cases corrective action must be taken.)

- Amdahl
- AT&T System V
- Data General DG/UX for AViiON Systems

VENDORS PROVIDING PATCHES

Cray Research, Inc. UNICOS 6.0/6.E/6.1 Field Alert #132 SPR 47600

For further information contact the Support Center at 1-800-950-CRAY or 612-683-5600 or e-mail support@crayamid.cray.com.

NeXT Computer, Inc. NeXTstep Release 2.x

A new version of rdist may be obtained from your authorized NeXT Support Center. If you are an authorized support center, please contact NeXT through your normal channels. NeXT also plans to make this new version of rdist available on the public NeXT FTP archives.

Silicon Graphics IRIX 3.3.x/4.0 (fixed in 4.0.1)

Patches may be obtained via anonymous ftp from sgi.com in the sgi/rdist directory.

Sun Microsystems, Inc. SunOS 4.0.3/4.1/4.1.1 Patch ID 100383-02

Patches may be obtained via anonymous ftp from ftp.uu.net or from local Sun Answer Centers worldwide.

The CERT/CC is hopeful that other patches will be forthcoming. We will be maintaining a status file, rdist-patch-status, on the cert.org system. We will add patch availability information to this file as it becomes known. The file is available via anonymous ftp to cert.org and is found in pub/cert_advisories/rdist-patch-status.

- ----------

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

Any user logged into the system can gain root access.

III. Solution

```
     A.  If available, install the appropriate patch provided by
         your operating system vendor.

     B.  If no patch is available, restrict the use of /usr/ucb/rdist
         by changing the permissions on the file.

         # chmod 711 /usr/ucb/rdist

- ----------------------------------------------------------------------------
The CERT/CC wishes to thank Casper Dik of the University of Amsterdam,
The Netherlands, for bringing this vulnerability to our attention.
We would also like to thank the vendors who have responded to this problem.
- ----------------------------------------------------------------------------

If you believe that your system has been compromised, contact CERT/CC via
telephone or e-mail.

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

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

Past advisories and other computer security related information are available
for anonymous ftp from the cert.org (192.88.209.5) system.

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

iQA/AwUBOBS9sFr9kb5qlZHQEQKchACeOzSpCg0b4+gdKcfTHwemySLVt4sAniYj
hQ2i849prtPJIrj5a5XJkcde
=ayZu
-----END PGP SIGNATURE-----
```