****
Security Bulletin 9723 DISA Defense Communications System
September 16, 1997 Published by: DISN Security Coordination Center
(SCC@NIC.MIL) 1-(800) 365-3642

DEFENSE INFORMATION SYSTEM NETWORK

SECURITY BULLETIN

The DISN SECURITY BULLETIN is distributed by the DISN SCC (Security Coordination Center) under DISA contract as a means of communicating information on network and host security exposures, fixes, and concerns to security and management personnel at DISN facilities. Back issues may be obtained via FTP from NIC.MIL [207.132.116.5] using login= “anonymous” and password=”guest”. The bulletin pathname is scc/sec-yynn (where “yy” is the year the bulletin is issued and “nn” is a bulletin number, e.g. scc/sec-9705.txt). These are also available at our WWW site, http://nic.mil.

****

+ - +
! !
! The following important advisory was issued by the Computer !
! Emergency Response Team (CERT) and is being relayed unedited !
! via the Defense Information Systems Agency’s Security !
! Coordination Center distribution system as a means of !
! providing DISN subscribers with useful security information. !
! !
+ - +

==========

CERT* Advisory CA-97.23
Original issue date: September 16, 1997
Last revised: --

Topic: Buffer Overflow Problem in rdist

- ----------

The CERT Coordination Center has received reports of a vulnerability in rdist that enables anyone with access to a local account to gain root privileges. This is not the same vulnerability as the one discussed in CA-96.14.

Section III.A contains instructions on how to determine if your site is

vulnerable. If your implementation of rdist is vulnerable, the CERT/CC team

encourages you to follow your vendor’s instructions (Sec. III.B and Appendix

A) or install a freely available version of the rdist program that is not installed as set-user-id root and is, therefore, not susceptible to the exploitation described in this advisory (Sec. III.C).

For information on the earlier problem with rdist, see
ftp://info.cert.org/pub/cert_advisories/CA-96.14.rdist_vul

We will update this advisory as we receive additional information. Please check our advisory files regularly for updates that relate to your site.

- ----------

I. Description

The rdist program is a UNIX Operating System utility used to distribute files from one host to another. On some systems, rdist opens network connections using a privileged port as the source port. This requires root privileges, and to attain these privileges rdist on such systems is installed set-user-id root.

A new vulnerability has been found in some set-user-id root implementations of rdist. The vulnerability lies in the function expstr(), where macros supplied as arguments are expanded using sprintf(). It is possible to overwrite stack frames and call specially pre-crafted native machine code. If the appropriate machine code is supplied, an attacker can execute arbitrary programs (such as the shell) with set-user-id root privileges.

Note that this vulnerability is distinct from that discussed in CERT advisory CA-96.14.

II. Impact

On systems with a vulnerable copy of rdist, anyone with access to a local account can gain root access.

III. Solution

We urge you to follow the steps in Section A to determine if your system is vulnerable and, if it is, to turn off rdist while you decide how to proceed.

If your system is vulnerable and you need the functionality that rdist provides, you should install a vendor patch (Section B). Until you can do so, you may want to use a freely available version of rdist that does not need to be installed as set-user-id root and is, therefore, not susceptible to the exploitation described in this advisory (Section C).

A. How to check for set-user-id root versions of rdist

To find set-user-id root versions of rdist and to disable the programs that are possibly vulnerable, use the following find command or a variant. Consult your local system documentation to determine how to tailor the find program on your system.

You will need to run the find command on each system you maintain because the command examines files on the local disk only.

Substitute the names of your local file systems for

FILE_SYSTEM_NAMES in the example. Example local file system names are /, /usr, and /var. You must do this as root.

Note that this is one long command, though we have separated it onto three lines using backslashes.

find FILE_SYSTEM_NAMES -xdev -type f -user root \

- name ‘*rdist*’ -perm -04000 -exec ls -l ‘{}’ \; \
- ok chmod 0500 ‘{}’ \;

This command will find all files on a system that

- are only in the file system you name (FILE_SYSTEM_NAMES -xdev)
- are regular files (-type f)
- are owned by root (-user root)
- have “rdist” as a component of the name (-name ‘*rdist*’)
- are setuid (-perm -04000)

Once found, those files will

- have their names and details printed (-exec ls -l ‘{}’)
- have the setuid mode removed (making the file available only to root) but only if you type `y’ in response to the prompt (-ok chmod 0500 ‘{}’ \;)

B. Obtain and install the appropriate patch

Below is a list of vendors who have provided information for this advisory. Details are in Appendix A, and we will update the appendix as we receive more information.

Berkeley Software Design, Inc. (BSDI)
Digital Equipment Corp.
FreeBSD, Inc.
Hewlett-Packard Company
IBM Corporation
NEC Corporation
The Santa Cruz Operation, Inc. (SCO)
Siemens-Nixdorf
Silicon Graphics Inc. (SGI)
Sun Microsystems, Inc.

If your vendor’s name is not on this list, please contact the vendor directly.

C. If you need the functionality that rdist provides but a patched version is not yet available from your vendor, consider installing rdist-6.1.3, which is freely available from

ftp://usc.edu/pub/rdist/rdist-6.1.3.tar.gz

MD5 (rdist-6.1.3.tar.gz) = 8a76b880b023c5e648b7cb77b9608b9f

The README file in the distribution explains how to configure and install this version of rdist.

We recommend that you configure this version of rdist to use rsh instead of rcmd. Here is the relevant text from the README:

By default rdist uses rsh(1c) to make connections to remote hosts. This has the advantage that rdist does not need to be setuid to “root”. This eliminates most potential security holes. It has the disadvantage that it takes slightly more time for rdist to connect to a remote host due to the added overhead of doing a fork() and then running the rsh(1c) command.

Some sites with sufficient expertise use the ssh program in conjunction with rdist, instead of using rcmd or rsh. If you have the expertise, you may want to implement this configuration.

For further details on this option see “Ssh (Secure Shell) FAQ - Frequently asked questions,” Section 4.4, “Can I use rdist with ssh?”

It is available from
http://www.uni-karlsruhe.de/~ig25/ssh-faq/ssh-faq-4.html
For details on how to obtain ssh, see FAQ Section 3.4, “Where can I
obtain ssh?” This section can be found in
http://www.uni-karlsruhe.de/~ig25/ssh-faq/ssh-faq-3.html

~~~~~~

Appendix A - Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor’s name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

==========
BSDI shipped a patch for this for our 2.1 release (U210-018) when the original Bugtraq advisory was released. The 3.0 version of rdist is not vulnerable and in fact is no longer even setuid.

Digital Equipment Corp.

==========
This reported problem is not present for Digital’s ULTRIX or Digital UNIX Operating Systems Software.

DIGITAL EQUIPMENT CORPORATION

FreeBSD, Inc.

==========
2.1.0 is vulnerable.

2.1.5, 2.1.6 and 2.1.7 are and 2.1-stable are not. In any case, upgrading to 2.1.7 or even better, 2.1-stable should be considered.

If there is demand, we’ll release a patch for 2.1.0

All 2.2 releases, 2.2-stable and FreeBSD-current are not vulnerable.

Hewlett-Packard Company

HP is -not- vulnerable; the problem didn’t exist in 9.X, and has been fixed in 10.X with Security Bulletin #36 (HPSBUX9608-036) last year. Patch numbers change frequently because of cumulative patching, so please check current patch ID information either by bulletin or by platform/release at our HP Electronic Support Center in the “Security Patch Matrix,” which is updated every 24 hours.

1) From your Web browser, access the URL:

   http://us-support.external.hp.com (US,Canada,Asia-Pacific, and Latin-America)

   http://europe-support.external.hp.com (Europe)

2) On the HP Electronic Support Center main screen, select the hyperlink “Support Information Digests”.

3) On the “Welcome to HP’s Support Information Digests” screen, under the heading “Register Now”, select the appropriate hyperlink “Americas and Asia-Pacific”, or “Europe”.
~~~~~~

4) On the “New User Registration” screen, fill in the fields for the User Information and Password and then select the button labeled “Submit New User”.
5) On the “User ID Assigned” screen, select the hyperlink “Support Information Digests”. **Note what your assigned user ID and password are for future reference.

6) You should now be on the “HP Support Information Digests Main” screen. You might want to verify that your email address is correct as displayed on the screen. From this screen, you may also view/subscribe to the digests, including the security bulletins digest.

   To get a patch matrix of current HP-UX and BLS security patches referenced by either Security Bulletin or Platform/OS, click on following screens in order:

Technical Knowledge Database
Browse the HP Security Bulletins Archive
HP-UX Security Patch Matrix

IBM Corporation

All versions of AIX are vulnerable to this buffer overflow. There is no 3.2 fix. It is recommended that 3.2 customers upgrade to a higher level. The following APARs will be available for AIX version 4 soon.

AIX 3.2: upgrade to 4.1.5 or higher
AIX 4.1: IX70876
AIX 4.2: IX70875

To Order

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL:

http://service.software.ibm.com/aixsupport/

or send e-mail to aixserv@austin.ibm.com with a subject of “FixDist”.

IBM and AIX are registered trademarks of International Business Machines Corporation.

NEC Corporation

The following systems are NOT affected by this vulnerability:

UX/4800
UX/4800(64)
EWS-UX/V(Rel4.2MP)
EWS-UX/V(Rel4.2)
UP-UX/V(Rel4.2MP)

To report a new vulnerability, contact <UX48-security-support@nec.co.jp>.

The Santa Cruz Operation, Inc. (SCO)

==========
SCO has determined that the following SCO operating systems are not vulnerable:

- SCO CMW+ 3.0
- SCO Open Desktop/Open Server 3.0
- SCO OpenServer 5.0
- SCO UnixWare 2.1

Siemens-Nixdorf Informationssysteme AG
Siemens-Nixdorf does not ship rdist.

Silicon Graphics Inc. (SGI)

==========
At this time, Silicon Graphics does not have any public information for the rdist buffer overflow issue. Silicon Graphics has communicated with CERT/CC and other external security parties and is actively investigating this issue. When more Silicon Graphics information (including any possible patches) is available for release, that information will be released via the SGI security mailing list, wiretap.

For subscribing to the wiretap mailing list and other SGI security related information, please refer to the Silicon Graphics Security Headquarters website located at:

http://www.sgi.com/Support/security/security.html

Sun Microsystems, Inc.

==========
We are producing patches.

- ----------

The CERT Coordination Center thanks Hiroshi Nakano of Ryukoku University, Japan for reporting this problem. We also thank Wolfgang Ley of DFN-CERT for his assistance with the Solutions section of the advisory.

- ----------

If you believe that your system has been compromised, contact the CERT Coordination Center or your representative in the Forum of Incident Response and Security Teams (see http://www.first.org/team-info/).

CERT/CC Contact Information

- ----------
Email cert@cert.org

Phone +1 412-268-7090 (24-hour hotline)
CERT personnel answer 8:30-5:00 p.m. EST(GMT-5) / EDT(GMT-4)
and are on call for emergencies during other hours.

Fax +1 412-268-6989

Postal address
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
USA

Using encryption

We strongly urge you to encrypt sensitive information sent by email. We can support a shared DES key or PGP. Contact the CERT/CC for more information.

Location of CERT PGP key
ftp://info.cert.org/pub/CERT_PGP.key
Getting security information
CERT publications and other security information are available from
http://www.cert.org/
ftp://info.cert.org/pub/

CERT advisories and bulletins are also posted on the USENET newsgroup
comp.security.announce
To be added to our mailing list for advisories and bulletins, send
email to
cert-advisory-request@cert.org
In the subject line, type
SUBSCRIBE your-email-address
- ----------

- ----------

This file: ftp://info.cert.org/pub/cert_advisories/CA-97.23.rdist
http://www.cert.org
click on “CERT Advisories”

~~~~~~

****
*
- The point of contact for NIPRNET security-related incidents is the
- ASSIST:
*
*
- E-mail address: ASSIST@ASSIST.MIL
*
*
- Telephone: 1-(800)-357-4231 (24 hours/day)
*
*
- You may also contact the Security Coordination Center (SCC) at the
*
- NIC:
*
*
- E-mail address: SCC@NIC.MIL
*
*
- Telephone: 1-(800)-365-3642
*
*
- NIC Help Desk personnel are available from 7:00 a.m.-7:00 p.m. EST,
*
- Monday through Friday except on federal holidays.
*
*
****

PLEASE NOTE: Some users outside of the DOD computing communities may receive DISN Security Bulletins. If you are not part of the DOD community, please contact your agency’s incident response
~~~~~~

team to report incidents. Your agency's team will coordinate with DOD. The Forum of Incident Response and Security Teams (FIRST) is a world-wide organization. A list of FIRST member organizations and their constituencies can be obtained by sending email to docserver@first.org with an empty subject line and a message body containing the line: send first-contacts.