CERT Advisory CA-1995-17 rpc.ypupdated Vulnerability

Original issue date: December 12, 1995
Last revised: October 30, 1997
Updated vendor information for Sun.

A complete revision history is at the end of this file.

The CERT Coordination Center has received reports of a vulnerability in the rpc.ypupdated program. An exploitation program has also been posted to several newsgroups.

This vulnerability allows remote users to execute arbitrary programs on machines that provide Network Information Service (NIS) master and slave services. Client machines of an NIS master or slave server are not affected.

See Section III for a test to help you determine if you are vulnerable, along with a workaround. In addition, Appendix A contains a list of vendors who have reported their status regarding this vulnerability.

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

I. Description

The rpc.ypupdated program is a server used to change NIS information from a network-based client using various methods of authentication.

Note:
The Network Information Service (NIS) was formerly known as Sun Yellow Pages (YP). The functionality of the two remains the same; only the name has changed. The name Yellow Pages is a registered trademark in the United Kingdom of British Telecommunications plc, and may not be used without permission.

Clients connect to rpc.ypupdated and provide authentication information and proposed changes to an NIS database. If authenticated, the information provided is used to update the selected NIS database.

The protocol used when clients communicate with a server only checks to see if the connection is authentic using secure RPC. The protocol does not check to see if the client is authorized to modify the NIS data or if the given NIS map exists. Even after an unsuccessful attempt to update the NIS information, the rpc.ypupdated server invokes the *make(1)* program to propagate possible changes. The invocation of make is implemented in an insecure fashion which allows the requesting client to pass malicious arguments to the call resulting in the execution of arbitrary commands on NIS master and slave servers.

II. Impact

Remote users can execute commands on vulnerable NIS master and slave machines.

III. Solution

First determine if you are vulnerable (see Sec. A below). If you are vulnerable, either follow the instructions vendors have provided in Appendix A or apply the workaround in Sec. B below.

1. Consult the vendor information in Appendix A.

   If your vendor is not listed, then check to see if your system has an rpc.ypupdated server. To do this check, consult your system documentation or look in your system initialization files (e.g., /etc/rc*, /etc/init.d/*, and inetd.conf) for rpc.ypupdated or ypupdated. If you find a reference to this program on your system, then it is likely that you are vulnerable.

1. Until patches are available for vulnerable systems, we recommend that you disable rpc.ypupdated as soon as possible.

   Below are some examples given for reference only. Consult your system documentation for the exact details.

   In these examples, the rpc.ypupdated program is killed if it is running, and the system is reconfigured so that the daemon does not automatically start again when the system is rebooted.

   Example 1 - SunOS 4.1.X
   For SunOS 4.1.X master and slave NIS servers, the rpc.ypupdated program is started by the /etc/rc.local script. First, determine if the server is running, and kill it if it is. Then, rename rpc.ypupdated so that the /etc/rc.local script will not find and therefore start it when the system reboots.

```
# /bin/uname -a
SunOS test-sun 4.1.4 1 sun4m
# /bin/ps axc | /bin/grep rpc.ypupdated
  108 ?  IW    0:00 rpc.ypupdated
# /bin/kill 108
# /bin/ps axc | /bin/grep rpc.ypupdated
# /bin/grep ypupdated /etc/rc /etc/rc.local
/etc/rc.local:  if [ -f /usr/etc/rpc.ypupdated -a -d /var/yp/$dname ]; then
/etc/rc.local:          rpc.ypupdated;  echo -n ' ypupdated'
# /bin/mv /usr/etc/rpc.ypupdated /usr/etc/rpc.ypupdated.CA-95.17
# /bin/chmod 0 /usr/etc/rpc.ypupdated.CA-95.17
```

Example 2 - IRIX
On IRIX systems, ypupdated is started by the inetd daemon. For versions 3.X, 4.X, 5.0.X, 5.1.X, and 5.2, the ypupdated is enabled; but for versions 5.3, 6.0.X, and 6.1, it is disabled. Note that the byte counts given for /bin/ed may vary from system to system. Note also that the inetd.conf file is found in different locations for different releases of IRIX. For 3.X and 4.X, it is located in /usr/etc/inetd.conf. For all other releases (5.0.X, 5.1.X, 5.2, 5.3, 6.0.X, and 6.1) it is in /etc/inetd.conf.

```
# /bin/uname -a
IRIX test-iris 5.2 02282015 IP20 mips
# /bin/grep ypupdated /etc/inetd.conf
ypupdated/1 stream rpc/tcp wait root /usr/etc/rpc.ypupdated ypupdated
# /bin/ps -eaf | /bin/grep rpc.ypupdated
    root   184     1  0   Nov 20 ?        0:00 /usr/etc/rpc.ypupdated
    root 14694 14610  2 11:30:07 pts/3    0:00 grep -i rpc.ypupdated
# /bin/kill 184
# /bin/ed /etc/inetd.conf
3344
/^ypupdated/s/^/#DISABLED# /p
#DISABLED# ypupdated/1 stream rpc/tcp wait root /usr/etc/rpc.ypupdated ypupdated
w
3355
q
# /bin/ps -eac | /bin/grep inetd
   193   TS  26 ?        0:04 inetd
# /bin/kill -HUP 193
```

Appendix A: Vendor Information

Below is information we have received from vendors. If you do not see your vendor's name below, please contact the vendor directly for information.

Apple Computer, Inc.

A/UX does not include this functionality and is therefore not vulnerable.

Berkeley Software Design, Inc. (BSDI)

BSD/OS by Berkeley Software Design, Inc. (BSDI) is not vulnerable.

Data General Corporation

Data General believes the DG/UX operating system to be NOT vulnerable. This includes all supported release, DG/UX 5.4 Release 3.10, DG/UX Release 4.10 and all related Trusted DG/UX releases.

Digital Equipment Corporation

OSF/1 on all Digital platforms is not vulnerable.

Digital ULTRIX platforms are not vulnerable to this problem.

Hewlett-Packard Company

HP-UX versions 10.01, 10.10, and 10.20 are vulnerable (versions prior to HP-UX 10.01 are not vulnerable).

Solution: Do not run rpc.ypupdated. rpc.ypupdated is used when adding or modifying the public:private key pair in the NIS map public key.byname via the chkey command interface. rpc.ypupdated should ONLY be run while changes are being made, then terminated when the changes are complete.
Make sure you re-kill rpc.ypupdated after each reboot.

IBM Corporation

AIX 3.2

APAR - IX55360
PTF - U440666

To determine if you have this PTF on your system, run the following command:

```
lslpp -lB U440666
```

AIX 4.1

APAR - IX55363

To determine if you have this fix on your system, run the following command:

```
lslpp -h | grep -p bos.net.nis.server
```

Your version of bos.net.nis.server should be 4.1.4.1 or later.

To Order

APARs may be ordered using FixDist or from the IBM Support Center. For more information on FixDist reference URL:

http://aix.boulder.ibm.com/pbin-usa/fixdist.pl/

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

NEC Corporation

OS	Version	Status
EWS-UX/V(Rel4.0)	R1.x - R2.x	not vulnerable
	R3.x - R6.x	vulnerable
EWS-UX/V(Rel4.2)	R7.x - R10.x	vulnerable
EWS-UX/V(Rel4.2MP)	R10.x	vulnerable
UP-UX/V	R2.x	not vulnerable
	R3.x - R4.x	vulnerable
UP-UX/V(Rel4.2MP)	R5.x - R7.x	vulnerable
UX/4800	R11.x	vulnerable

The following is a workaround for 48 series.

ypupdated program is started by the /etc/rc2.d/S75rpc script. First, determine if the server is running, killing it if it is. Then, rename ypupdated so that the /etc/rc2.d/S75rpc script will not find and therefore start it when the system reboots.

```
# uname -a
UNIX_System_V testux 4.2 1 R4000 r4000
# /sbin/ps -ef | /usr/bin/grep ypupdated
    root   359     1  0 08:20:05 ?        0:00 /usr/lib/netsvc/yp/ypupdated
    root 19938   836  0 23:13:20 pts/1    0:00 /usr/bin/grep ypupdated
# /usr/bin/kill 359
# /sbin/mv /usr/lib/netsvc/yp/ypupdated /usr/lib/netsvc/yp/ypupdated.CA-95.17
# /usr/bin/chmod 0 /usr/lib/netsvc/yp/ypupdated.CA-95.17
```

Contacts for further information:
E-mail:UX48-security-support@nec.co.jp

Open Software Foundation

YP/NIS is not part of the OSF/1 Version 1.3 offering.
Hence, OSF/1 Version 1.3 is not vulnerable.

Sequent Computer Systems

Sequent does not support the product referred to in this advisory, and as such is not vulnerable.

Silicon Graphics Inc. (SGI)

IRIX 3.x, 4.x, 5.0.x, 5.1.x, 5.2: vulnerable.
Turn off rpc.ypudated in inetd.conf; it is shipped with this turned on.

IRIX 5.3, 6.0, 6.0.1: rpc.ypupdated was off as distributed.
Turn off if you have turned it on.

Solbourne

Not vulnerable.

Sun Microsystems, Inc.

BUG 1230027/1232146 fixed in 4.1.3, will not fix 2.4

The ypupdated program is no longer shipped with NS-KIT. If we do decide in the future to support it again, we will fix the bug.

Revision History

```
Oct. 30, 1997  Updated vendor information for Sun.
Sep. 23, 1997  Updated copyright information
Aug. 30, 1996  Information previously in the README was inserted
               into the advisory.
Feb. 21, 1996  Appendix, IBM - added an entry for IBM
Dec. 18, 1995  Appendix, Digital & Hewlett-Packard - modified information
```