CERT Advisory CA-1994-15 NFS Vulnerabilities

Original issue date: December 19, 1994
Last revised: Septmeber 23, 1997
Updated copyright statement

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

The CERT Coordination Center is experiencing an increase in reports of root compromises caused by intruders using tools to exploit a number of NFS (Network File System) vulnerabilities.

CERT recommends limiting your exposure to these attacks by implementing the security measures described in Section III below.

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

I. Description
There are tools being used by intruders to exploit a number of NFS vulnerabilities. These tools are widely available and widely distributed.

II. Impact
The impact varies depending on which vulnerabilities are present. In the worst case, intruders gain unauthorized root access from a remote host.

III. Security Measures

A. Filter packets at your firewall/router.
Filter TCP port 111, UDP port 111 (portmapper), TCP port 2049, and UDP port 2049 (nfsd).

Note: Some sites may run NFS on a port other than 2049. To determine which port is running NFS, enter the following command on the machine in question:

```
rpcinfo -p
```

If NFS is on a different port, then that is the port number to block at the firewall.

Consult your vendor or your firewall documentation for detailed instructions on how to configure the ports.

This measure will prevent access to NFS at your site from outside your firewall, but it will not protect you from attacks launched from your local network, behind your firewall.

B. Use a portmapper that disallows proxy access.
Be sure that you do this for every host that runs a portmapper. For Solaris, 2.x, use a version of rpcbind that disallows proxy access.

A portmapper that disallows proxy access protects all hosts with the modified portmapper from attacks that originate either inside or outside your firewall. Because this security measure addresses only the portmapper vulnerability, we recommend combining it with measure A above. Wietse Venema has developed a portmapper that disallows proxy access. It is available by anonymous FTP from

```
ftp.win.tue.nl: /pub/security/portmap_3.shar.Z
ftp.cert.org:   /pub/tools/nfs_tools/portmap_3.shar.Z
MD5 checksum:   f6a3ad98772e7a402ddcdac277adc4a6
```

For Solaris systems, Venema has developed a version of rpcbind that does not allow proxy access. Solaris users should install this program, not the portmapper. Rpcbind is available by anonymous FTP from the same sites as the portmapper:

```
ftp.win.tue.nl:/pub/security/rpcbind_1.1.tar.Z
ftp.cert.org:  /pub/tools/nfs_tools/rpcbind_1.1.tar.Z
MD5 checksum:  58437adcbea0a55e37d3a3211f72c08b
```

C. Check the configuration of the /etc/exports files on your hosts.
In particular:

1. Do *not* self-reference an NFS server in its own exports file.
2. Do not allow the exports file to contain a "localhost" entry.
3. Export file systems only to hosts that require them.
4. Export only to fully qualified hostnames.
5. Ensure that export lists do not exceed 256 characters.
   If you have aliases, the list should not exceed 256 characters *after* the aliases have been expanded.
   (See CA-94.02.REVISED.SunOS.rpc.mountd.vulnerability)
6. Use the *showmount(8)* utility to check that exports are correct.
7. Wherever possible, mount file systems to be exported read only and export file systems read only.

D. Ensure that your systems are current with patches and workarounds available from your vendor and identified in CERT advisories.

The following advisories address problems related to NFS:

CA-91.21.SunOS.NFS.Jumbo.and.fsirand
CA-92.12.REVISED.SunOS.rpc.mountd.vulnerability
CA-93.15.SunOS.and.Solaris.vulnerabilities
CA-94.02.REVISED.SunOS.rpc.mountd.vulnerability

Vendors may have additional patches not covered by a CERT advisory, so be sure to contact your vendor for further information.

The CERT Coordination Center thanks Steve Bellovin, Casper Dik, Leendert van Doorn, and Wietse Venema for their support in responding to this problem.

Revision History

```
Sep. 23, 1997  Updated copyright statement
Aug. 30, 1996  Information previously in the README was inserted
               into the advisory.
Feb. 02, 1995  Sec. III - Added a note about checking port numbers.
```