**********

DDN Security Bulletin 06 DCA DDN Defense Communications System
1 Nov 89 Published by: DDN Security Coordination Center
(SCC@NIC.DDN.MIL) (800) 235-3155

DEFENSE DATA NETWORK
SECURITY BULLETIN

The DDN SECURITY BULLETIN is distributed by the DDN SCC (Security Coordination Center) under DCA contract as a means of communicating information on network and host security exposures, fixes, & concerns to security & management personnel at DDN facilities. Back issues may be obtained via FTP (or Kermit) from NIC.DDN.MIL [26.0.0.73 or 10.0.0.51] using login="anonymous" and password="guest". The bulletin pathname is SCC:DDN-SECURITY-nn (where "nn" is the bulletin number).

**********

## SUN RCP VULNERABILITY

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

### CERT Advisory

October 26, 1989

### Sun RCP vulnerability

A problem has been discovered in the SunOS 4.0.x rcp. If exploited, this problem can allow users of other trusted machines to execute root-privilege commands on a Sun via rcp.

This affects only SunOS 4.0.x systems; 3.5 systems are not affected.

A Sun running 4.0.x rcp can be exploited by any other trusted host listed in /etc/hosts.equiv or /.rhosts. Note that the other machine exploiting this hole does not have to be running Unix; this vulnerability can be exploited by a PC running PC/NFS, for example.

This bug will be fixed by Sun in version 4.1 (Sun Bug number 1017314),
but for now the following workaround is suggested by Sun:

Change the 'nobody' /etc/passwd file entry from

nobody:*:-2:-2::/:

to

nobody:*:32767:32767:Mismatched NFS ID's:/nonexistant:/nosuchshell

If you need further information about this problem, please contact
CERT by electronic mail or phone.

J. Paul Holbrook
Computer Emergency Response Team (CERT)
Carnegie Mellon University
Software Engineering Institute

Internet: <cert@SEI.CMU.EDU>
(412) 268-7090 (24 hour hotline)
**********