```
**********************************************************************
DDN Security Bulletin 05         DCA DDN Defense Communications System
23 Oct 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).

****

ULTRIX 3.0 BREAK-IN ATTEMPTS

```
+ - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - +
!  Although there are only thirteen MILNET sites running any version of   !
!  Ultrix, the SCC is forwarding this CERT Advisory as an aid to those    !
!  Internet sites which may be affected.  Note that these problems        !
!  have affected only sites running Ultrix 3.0.                           !
+ - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - +
```

CERT Advisory
DEC/Ultrix 3.0 Systems

Recently, the CERT/CC has been working with several Unix sites that have experienced break-ins. The bulk of the problems have stemmed from hosts running tftpd, accounts with guessable passwords or no passwords, and known security holes not being patched.

The intruder, once in, gains root access and replaces key programs with ones that create log files which contain accounts and passwords in clear text. The intruder then returns and collects the file. By using accounts which are trusted on other systems, the intruder then installs replacement programs which start logging.

There have been many postings about the problem from several other net users. In addition to looking for setuid root programs in users' home directories, hidden directories '.. ' (dot dot space space), and a modified telnet program, we have received two reports from Ultrix 3.0 sites that the intruders are replacing the /usr/bin/login program. The Ultrix security hole being used in these attacks is only found in Ultrix 3.0.

Suggested steps:

1) Check for a bogus /usr/bin/login. The sum program reports:
   27379 67 for VAX/Ultrix 3.0

2) Check for a bogus /usr/etc/telnetd. The sum program reports:
   23552 47 for VAX/Ultrix 3.0

3) Look for .savacct in either /usr/etc or in users' directories. This may be the file that the new login program creates. It could have a different name on your system.

4) Upgrade to Ultrix 3.1 ASAP.

5) Monitor accounts for users having passwords that can be found in the /usr/dict/words file or have simple passwords like a persons name or their account name.

6) Search through the file system for programs that are setuid root.

7) Disable or modify the tftpd program so that anonymous access to the file system is prevented.

If you find that a system that has been broken into, changing the password on the compromised account is not sufficient. The intruders do remove copies of the /etc/passwd file in order to break the remaining passwords. It is best to change all of the passwords at one time. This will prevent the intruders from using another account.

Please alert CERT if you do find a problem:

Computer Emergency Response Team
Email: cert@sei.cmu.edu
Telephone: 412-268-7090 (answers 24 hours a day)

For general questions, contact the SCC:

DDN Security Coordination Center
Email: scc@nic.ddn.mil
Telephone: 800-235-3155 (7 a.m. to 5 p.m. Pacific time)

****