CERT Advisory CA-1993-04 Commodore Amiga UNIX finger Vulnerability

Original issue date: February 18, 1993
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file. **THIS IS A REVISED CERT ADVISORY**
IT CONTAINS UPDATED INFORMATION

The CERT Coordination Center has received information concerning a vulnerability in the "finger" program of Commodore Business Machine's Amiga UNIX product. The vulnerability affects Commodore Amiga UNIX versions 1.1, 2.03, 2.1, 2.1p1, 2.1p2, and 2.1p2a. Commodore is aware of the vulnerability, and both a workaround and a patch are available. Affected sites should apply either the workaround or the patch, and directions are provided below.

The Commodore contact e-mail address given in CERT Advisory CA-93.04 was incorrect. This revised advisory provides the correct e-mail address. If you have any further questions, contact David Miller of Commodore via e-mail at davidm@commodore.com .

I. Description

The "finger" command in Amiga UNIX contains a security vulnerability.

II. Impact

Non-privileged users can gain unauthorized access to files.

III. Solution

Commodore has suggested a workaround and a patch, as follows:

1. Workaround
   As root, modify the permission of the existing /usr/bin/finger to prevent misuse.

   ```
   # /bin/chmod 0755 /usr/bin/finger
   ```

1. Patch

   As root, install the "pubsrc" package from the distribution tape.

   In the file, "/usr/src/pub/cmd/finger/src/finger.c", add the line:

   ```
   setuid(getuid());
   ```

   immediately before the line reading:

   ```
   display_finger(finger_list);
   ```

   (Optionally) save a copy of the existing /usr/bin/finger and modify its permission to prevent misuse.

   ```
   # /bin/mv /usr/bin/finger /usr/bin/finger.orig
   # /bin/chmod 0755 /usr/bin/finger.orig
   ```

   In the directory, "/usr/src/pub/cmd/finger", issue the command:

   ```
   # cd /usr/src/pub/cmd/finger
   # make install
   ```

The CERT Coordination Center wishes to thank Commodore Business Machines for their response to this problem.

Revision History

```
September 19,1997 Attached Copyright Statement
```