CERT Advisory CA-1991-11 ULTRIX LAT/Telnet Gateway Vulnerability

Original issue date: August 14, 1991
Last revised: September 18, 1997
Attached copyright statement

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

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability in LAT/Telnet gateway software in Digital Equipment Corporation's (DEC) ULTRIX versions 4.1 and 4.2 on all architectures. Information regarding the exploitation of this vulnerability has been publicly disclosed so we recommend taking immediate action. Until you are able to apply the patch we recommend that sites disable the LAT/telnet service.

DEC has made a patch available which consists of new /usr/ucb/telnet binaries.

The patch is available through DEC's Customer Support Centers. Sites within the USA should call 1-800-525-7100. Sites in Europe and elsewhere should contact DEC through their normal channels.

I. Description

A vulnerability exists such that ULTRIX 4.1 and 4.2 systems running the LAT/Telnet gateway software can allow unauthorized privileged access. Although you may not be running the LAT/Telnet service at this time, the CERT/CC urges all sites to install the patch. This will ease any future installation of the gateway software.

The LAT/Telnet software requires special installation and is NOT part of the default ULTRIX configuration.

II. Impact

Anyone who can access a terminal or modem connected to the LAT server running the LAT/Telnet service can gain unauthorized root privileges.

III. Solution

Obtain the appropriate version of the patch kit for your system architecture from your DEC Customer Support Center, and install according to the accompanying instructions.

The CERT/CC would like to thank George Michaelson of The Prentice Centre, University of Queensland, Australia and John Annen of Davidson College for bringing this to our attention. We would also like to thank DEC for their response to this vulnerability and CIAC for their assistance.

Revision History

```
September 18,1997  Attached Copyright Statment
```