

CERT Advisory CA-1991-17 DECnet-Internet Gateway Vulnerability

Original issue date: September 26, 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 the configuration of the DECnet-Internet gateway software for Digital Equipment Corporation's (DEC) ULTRIX versions 4.0, 4.1, and 4.2 on all Digital architectures.

Digital Equipment Corporation is aware of this problem and a resolution for this vulnerability will be included in a future release. Digital and the CERT/CC strongly recommend that sites exposed to this vulnerability immediately institute the workaround detailed in this advisory.

I. Description

When installing the DECnet-Internet gateway software it is necessary to create a guest account on the ULTRIX gateway host. By default, this account has `/bin/csh` as its shell. By virtue of the guest account having a valid shell, the DECnet-Internet gateway software can be exploited to allow unauthorized root access.

II. Impact

Anyone using the DECnet-Internet gateway can gain unauthorized root privileges on the ULTRIX gateway host.

III. Solution

This section describes a workaround for this vulnerability. Disable the guest account by editing the `/etc/passwd` file and setting the shell field for the guest account to `/bin/false`. Also, ensure the guest account has the string "NoLogin" in the password field as detailed in the DECnet-Internet installation manual. Even if you have not installed or are not running the DECnet- Internet gateway software, Digital recommends that you implement the workaround solution stated above.

The CERT/CC wishes to thank R. Scott Butler of the Du Pont Company for bringing this vulnerability to our attention and for his further assistance with the temporary workaround.

Copyright 1991 Carnegie Mellon University.

Revision History

September 18,1997 Attached Copyright Statement