CERT Advisory CA-1996-13 Vulnerability in the dip program

Original issue date: July 9, 1996
Last revised: September 24, 1997
Updated copyright statement

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

The CERT Coordination Center has received several reports of exploitations of a vulnerability in the dip program on Linux systems. The dip program is shipped with most versions of the Linux system; and versions up to and including version 3.3.7n are vulnerable. An exploitation script for Linux running on X86-based hardware is publicly available. Although exploitation scripts for other architectures and operating systems have not yet been found, we believe that they could be easily developed.

The CERT Coordination Center recommends that you disable dip and re-enable it only after you have installed a new version. Section III below describes how to do that.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

dip is a freely available program that is included in most distributions of Linux. It is possible to build it for and use it on other UNIX systems.

The dip program manages the connections needed for dial-up links such as SLIP and PPP. It can handle both incoming and outgoing connections. To gain access to resources it needs to establish these IP connections, the dip program must be installed as set-user-id root.

A vulnerability in dip makes it possible to overflow an internal buffer whose value is under the control of the user of the dip program. If this buffer is overflowed with the appropriate data, a program such as a shell can be started. This program then runs with root permissions on the local machine.

Exploitation scripts for dip have been found running on Linux systems for X86 hardware. Although exploitation scripts for other architectures and operating systems have not yet been found, we believe that they could be easily developed.

II. Impact

On a system that has dip installed as set-user-id root, anyone with access to an account on that system can gain root access.

III. Solution

Follow the steps in Section A to disable your currently installed version of dip. Then, if you need the functionality that dip provides, follow the steps given in Section B.

A. Disable the presently installed version of dip.

As root,

```
chmod 0755 /usr/sbin/dip
```

By default, dip is installed in the /usr/sbin directory. Note that it may be installed elsewhere on your system.

B. Install a new version of dip.

If you need the functionality that dip provides, retrieve and install the following version of the source code for dip, which fixes this vulnerability. dip is available from

ftp://sunsite.unc.edu/pub/Linux/system/Network/serial/dip/dip337o-uri.tgz
ftp://sunsite.unc.edu/pub/Linux/system/Network/serial/dip/dip337o-uri.tgz.sig

MD5 (dip337o-uri.tgz) = 45fc2a9abbcb3892648933cadf7ba090
SHash (dip337o-uri.tgz) = 6e3848b9b5f9d5b308bbac104eaf858be4dc51dc

---

The CERT Coordination Center staff thanks Uri Blumenthal for his solution to the problem and Linux for their support in the development of this advisory.

Revision History

```
Sep. 24, 1997 Updated copyright statement
Aug. 30, 1996 Removed references to CA-96.13.README.
```