lpr-wrapper v.1.01

(first public release)

CERT issued an advisory (*) on 25 Junr 1997 that 'lpr' can be mis-used to gain root access or execute commands as root.

NeXT fixed this hole in **`4.2`**, but that doesn't help those of us who can't afford quarterly bux-fixes at **`$300`** a pop (if you are academic).

This wrapper is supposed to prevent this abuse, by renaming the old version to 'lpr.orig' and then set the new version to 'lpr'

If you have the developer tools, you can get this:

`ftp://ftp.auscert.org.au/pub/auscert/tools/overflow_wrapper/overflow_wrapper.c`

and compile it.

All I did was download it and rename 'overflow_wrapper.c' to 'lpr.c' and then I compiled it using:

```
cc -arch m68k -arch i386 -arch hppa -arch sparc \
-DREAL_PROG='"/usr/ucb/lpr.orig"' -DMAXARGLEN=32 -DSYSLOG -o lpr lpr.c
```

Then I stripped it.

Note: the 'syslog' part means that it will log any failed attempts to overrun the buffer.

With the help of **PackageBuilder.app** by Joakim Johansson <d91-jjo@nada.kth.se> and **Rex Dieter** <rdieter@math.unl.edu> (*who helped me understand the finer points of building packages and helped improve and debug the install/deinstall scripts*) I figured out how to turn this into a Installer .pkg (my first :-)

Permissions are vitally important here.

The original 'lpr' ships like this:

```
   -rws--s--x   1 root     daemon   /usr/ucb/lpr
```

The wrapper should have these permissions and the original lpr should be renamed 'lpr.orig'

```
-r-x--x--x   1 root     wheel    /usr/ucb/lpr.orig
```

Note: the first time this installation program runs it makes a backup of the original 'lpr' at '/usr/ucp/lpr.distribution' (with secure permissions) in case anything goes wrong with the installation procedure.

(*) The original CERT advisory should have been provided with this package. If it was not, you can find it here:

```
ftp://info.cert.org/pub/cert_advisories/CA-97.19.bsdlp
```

If you have any questions, please